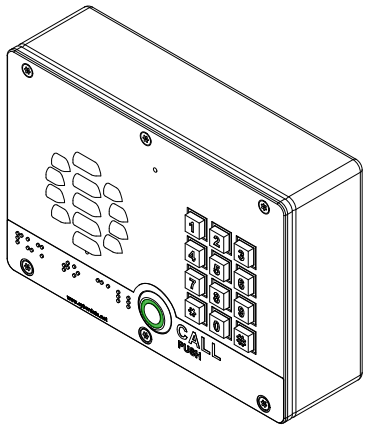
CyberData

The IP Endpoint Company



VoIP V3 Outdoor Intercom with Keypad Operations Guide

Part #011214

Document Part #*930522C*
for Firmware Version *7.1.7*

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

PoE VoIP Intercom Operations Guide 930522C
Part # 011214

COPYRIGHT NOTICE:
© 2012, CyberData Corporation, ALL RIGHTS RESERVED.

This manual and related materials are the copyrighted property of CyberData Corporation. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this manual, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.

CyberData
The IP Endpoint Company

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
http://www.cyberdata.net/support/contactsupportvoip.html

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Pictorial Alert Icons

GENERAL ALERT	General Alert *This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.*
	Ground *This pictoral alert indicates the Earth grounding connection point.*

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

Revision Information

Revision 930522C, which corresponds to firmware version 7.1.7, was released on December 17, 2012 and has the following changes:

- Updates Section 1.3, "Product Features".
- Adds Figure 1-3, "Unit Dimensions and Intrusion Sensor Range without the Gang Box".
- Adds Figure 1-4, "PCB Dimensions and Intrusion Sensor Range".
- Adds Figure 2-1, "Intercom Components".
- Updates Figure 2-3, "Intercom Connections".
- Updates Section 2.3.2, "Connecting the Intercom to the Auxiliary Relay".
- Updates Figure 2-4, "Auxiliary Relay Wiring Diagram".
- Updates Appendix A, “Mounting the VoIP V3 Outdoor Intercom with Keypad”.
- Adds Figure A-2, "Unit Dimensions—Rear View with Mounting Hole Locations".

Contents

Chapter 1 Product Overview 1

1.1 How to Identify This Product 1
1.2 Typical System Installation 2
1.3 Product Features 3
1.4 Supported Protocols 4
1.5 Supported SIP Servers 4
1.6 Product Specifications 5
1.7 Dimensions 6

Chapter 2 Installing the VoIP V3 Outdoor Intercom with Keypad 9

2.1 Parts List 9
2.2 Intercom Components 10
2.2.1 Call Button and Indicator Light 11
2.2.2 Dialing from the Keypad 11
2.3 Intercom Setup 12
2.3.1 Intercom Connections 12
2.3.2 Connecting the Intercom to the Auxiliary Relay 13
2.3.3 Identifying the Connector Locations and Functions 15
2.3.4 Network Connectivity, and Data Rate 18
2.3.5 RTFM Button 19
2.3.6 Adjust the Volume 20
2.4 Configure the Intercom Parameters 21
2.4.1 Factory Default Settings 21
2.4.2 Intercom Web Page Navigation 22
2.4.3 Log in to the Configuration Home Page 23
2.4.4 Configure the Device Parameters 26
2.4.5 Configure the Network Parameters 29
2.4.6 Configure the SIP Parameters 31
2.4.7 Configure the Button Parameters 35
2.4.8 Configure the Night Ringer Parameters 41
2.4.9 Configure the Sensor Parameters 43
2.4.10 Configure the Multicast Parameters 46
2.4.11 Configure the Audio Parameters 48
2.4.12 Configure the Event Parameters 54
2.4.13 Configure the Autoprovisioning Parameters 59
2.5 Upgrade the Firmware and Reboot the Intercom 63
2.5.1 Reboot the Intercom 65
2.6 Command Interface 66
2.6.1 Command Interface Post Commands 66

Appendix A Mounting the VoIP V3 Outdoor Intercom with Keypad 70

A.1 Mount the Intercom 70
A.2 Dimensions 71
A.3 Overview of Installation Types 75
A.4 Network Cable Entry Restrictions 76
A.4.1 Rear Conduit Network Cable Entry Restrictions (without Shroud) 76
A.4.2 Rear Conduit Network Cable Entry Restrictions (with Shroud) 76
A.5 Service Loop Cable Routing 77
A.6 Securing the Intercom 78
A.7 Additional Mounting Options 79
A.7.1 Rear Conduit Mounting Option (Not Provided) 79
A.7.2 Concrete Wall Mounting Option (Not Provided) 80
A.7.3 Goose Neck Mounting Option (Not Provided) 81

Appendix B Setting up a TFTP Server 82

B.1 Set up a TFTP Server 82

B.1.1 In a LINUX Environment 82
B.1.2 In a Windows Environment 82

Troubleshooting/Technical Support 83

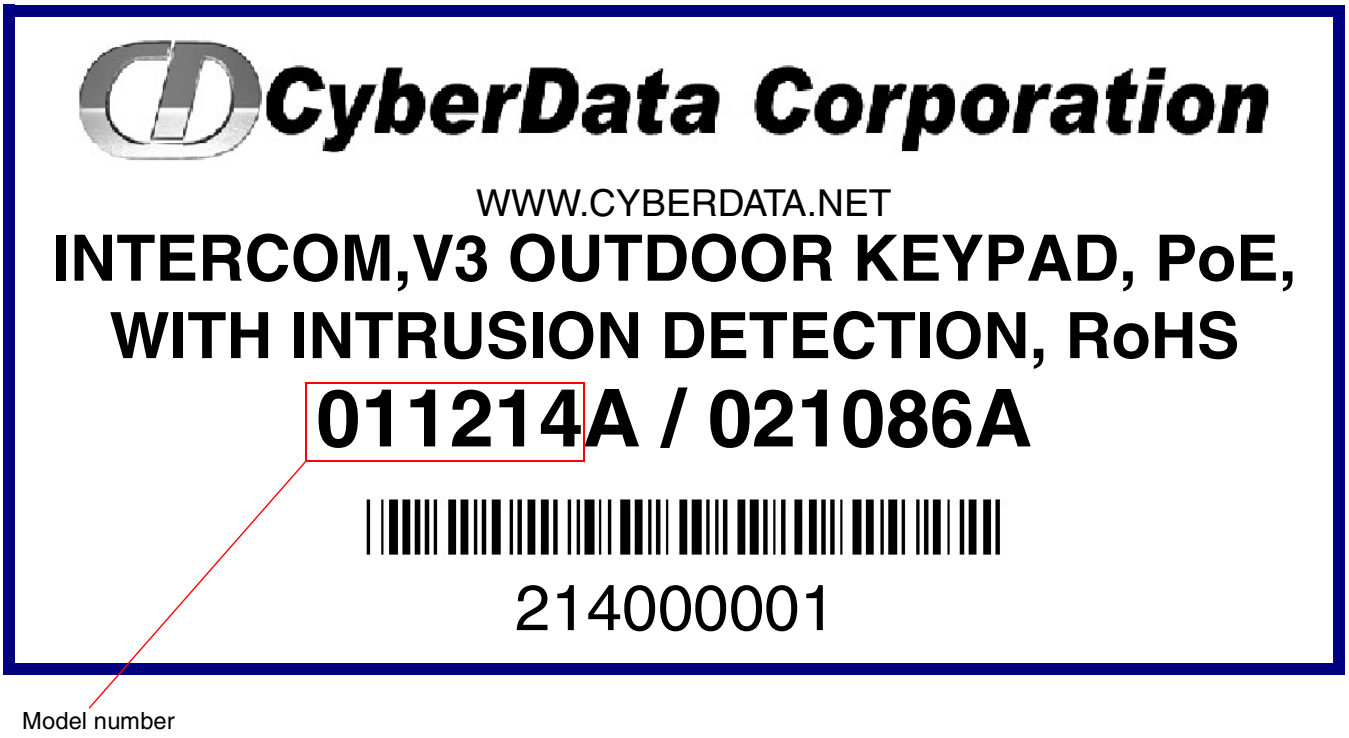
C.1 Frequently Asked Questions (FAQ) 83
C.2 Documentation 83
C.3 Contact Information 84
C.4 Warranty 85
C.4.1 Warranty & RMA Returns within the United States 85
C.4.2 Warranty & RMA Returns Outside of the United States 85
C.4.3 Spare in the Air Policy 85
C.4.4 Return and Restocking Policy 86
C.4.5 Warranty and RMA Returns Page 86

1 Product Overview

1.1 How to Identify This Product

To identify the VoIP V3 Outdoor Intercom with Keypad, look for a model number label similar to the one shown in Figure 1-1. The model number on the label should be **011214**.

Figure 1-1. Model Number Label

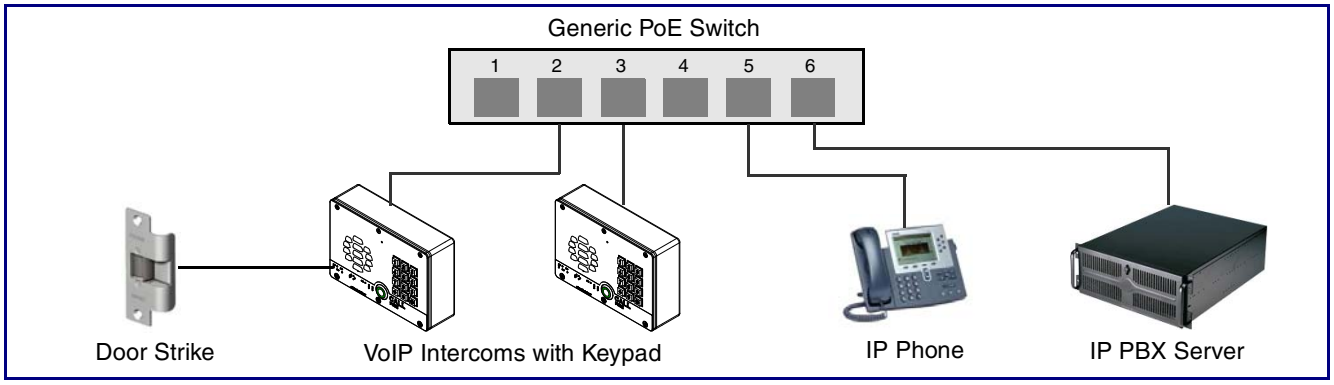


1.2 Typical System Installation

The Voice-over-IP (VoIP) Intercom is a Power-over-Ethernet (PoE 802.3af) and Voice-over-IP (VoIP) two-way communications device that easily connects into existing local area networks (LANs) with a single cable connection. The intercom is compatible with most SIP-based IP PBX servers that comply with SIP RFC 3261.

Figure 1-2 illustrates how the VoIP V3 Outdoor Intercom with Keypad can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation—Door Entry/Access Control



.

GENERAL ALERT	Warning *Electrical Hazard:* The VoIP Intercom enclosure is not rated for any AC voltages.
GENERAL ALERT	Warning *Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.
GENERAL ALERT	Warning *Electrical Hazard:* To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

1.3 Product Features

The VoIP V3 Outdoor Intercom with Keypad has the following features:

- 12-key keypad with backlight
- Programmable speed dial
- Optional Weather Shroud for even greater weather protection
- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment. SRST parameters are entered statically into the CyberData product's internal webpage.
- SIP
- Dual speeds of 10 Mbps and 100 Mbps
- 802.3af compliant
- 2 gang outlet box size
- Adaptive full duplex voice operation
- Network/Web management
- Network adjustable speaker volume adjustment
- Network configurable door or intrusion sensor settings
- Network configurable relay activation settings
- Dial Out Extension supports the addition of comma delimited pauses before sending additional DTMF tones
- Network configurable microphone input sensitivity adjustment
- Network downloadable product firmware
- Doubles as a paging speaker
- Call button
- Call activity indicator (light)
- Tamper proof design
- One dry contact relay for auxiliary control

Note The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

- Autoprovisioning
- Configurable audio files
- Night Ringer
- Three year warranty
- Peer-to-peer capable
- Door closure and tamper alert signal
- Optional Torx screws with driver kit
- An active call is indicated by the Call Button LED blinking at one second intervals.

1.4 Supported Protocols

The Intercom supports:

- SIP
- HTTP Web-based configuration
- Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- DHCP Client
- Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client
- Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- RTP/AVP - Audio Video Profile
- Audio Encodings

  PCMU (G.711 mu-law)

  PCMA (G.711 A-law)

  Packet Time 20 ms

1.5 Supported SIP Servers

The following link contains information on how to configure the Intercom for the supported SIP servers:

http://www.cyberdata.net/support/voip/server.html

1.6 Product Specifications

Category	Specification
Output	1 Watt Peak Power
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +12 to 24 VDC at 1000 mA (500 mA minimum)
Operating Temperature	-30 to 55 C (-22 to 131 F)
Payload Types	G711, A-law and µ-law
Regulatory Compliance	FCC Class A, UL 60950
Dimensions	6.5” x 4.5” x 1.5” (H x W x D)
Warranty	2 years limited
Part Number	011214
	011215 Weather Shroud (sold separately)
Auxiliary Relay	1A at 30 VDC

1.7 Dimensions

Figure 1-1. Unit Dimensions—Front and Side View

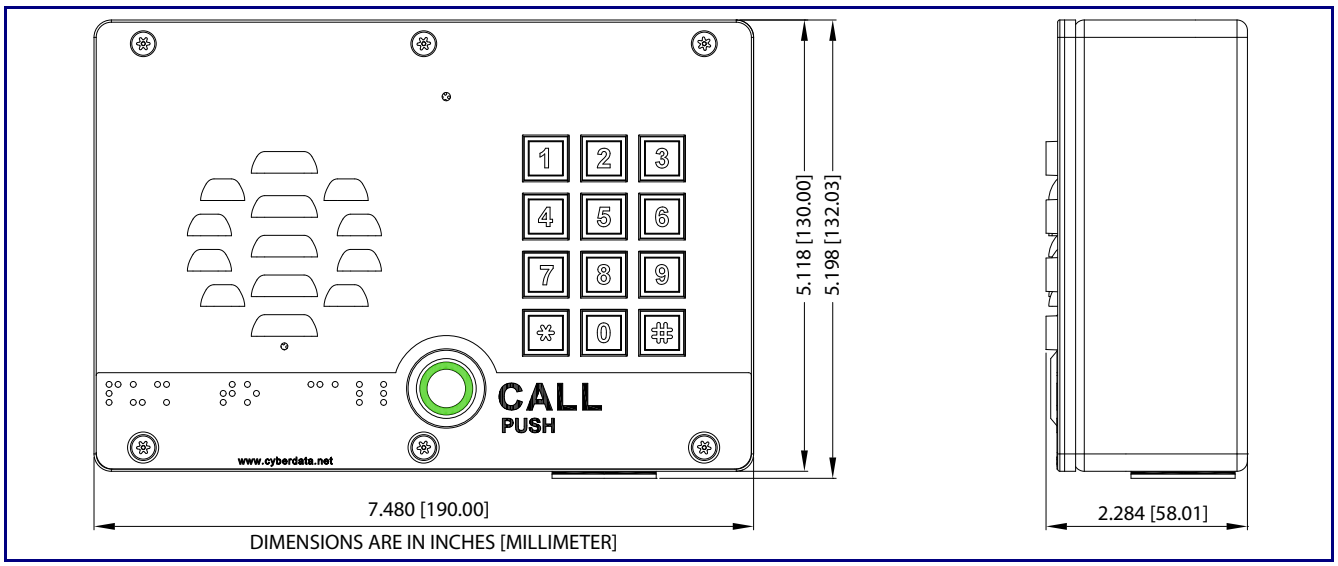


Figure 1-2. Shroud Dimensions and Mounting Hole Locations

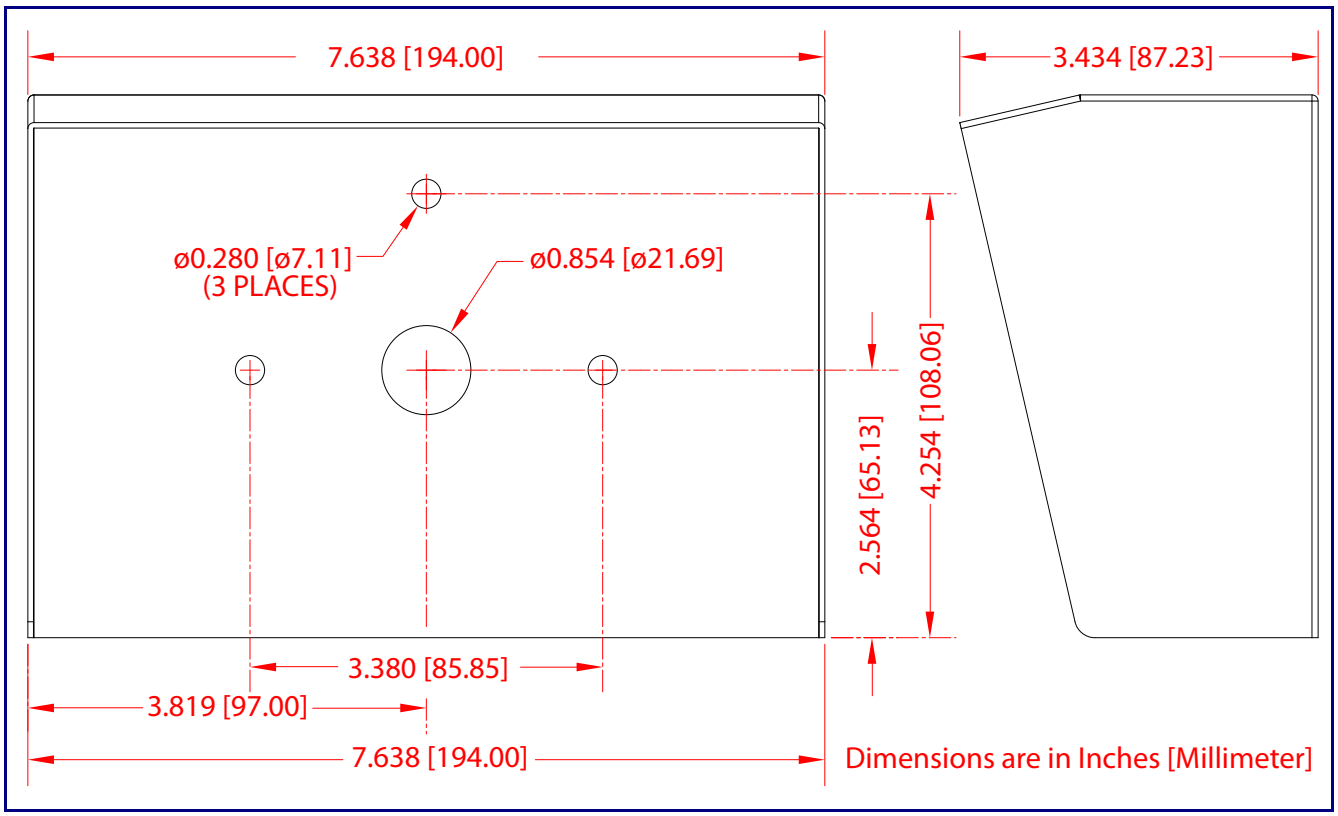


Figure 1-3. Unit Dimensions and Intrusion Sensor Range without the Gang Box

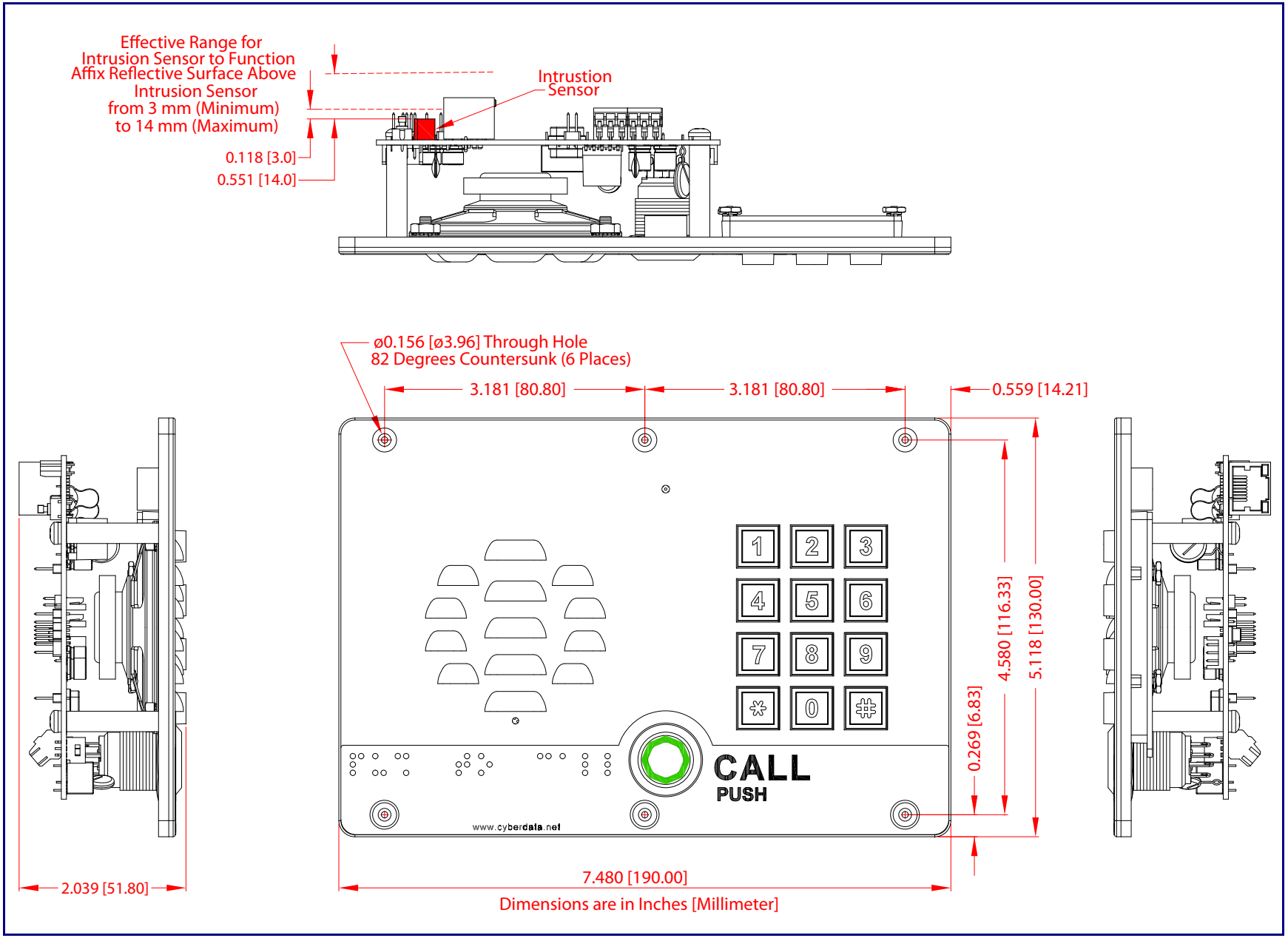
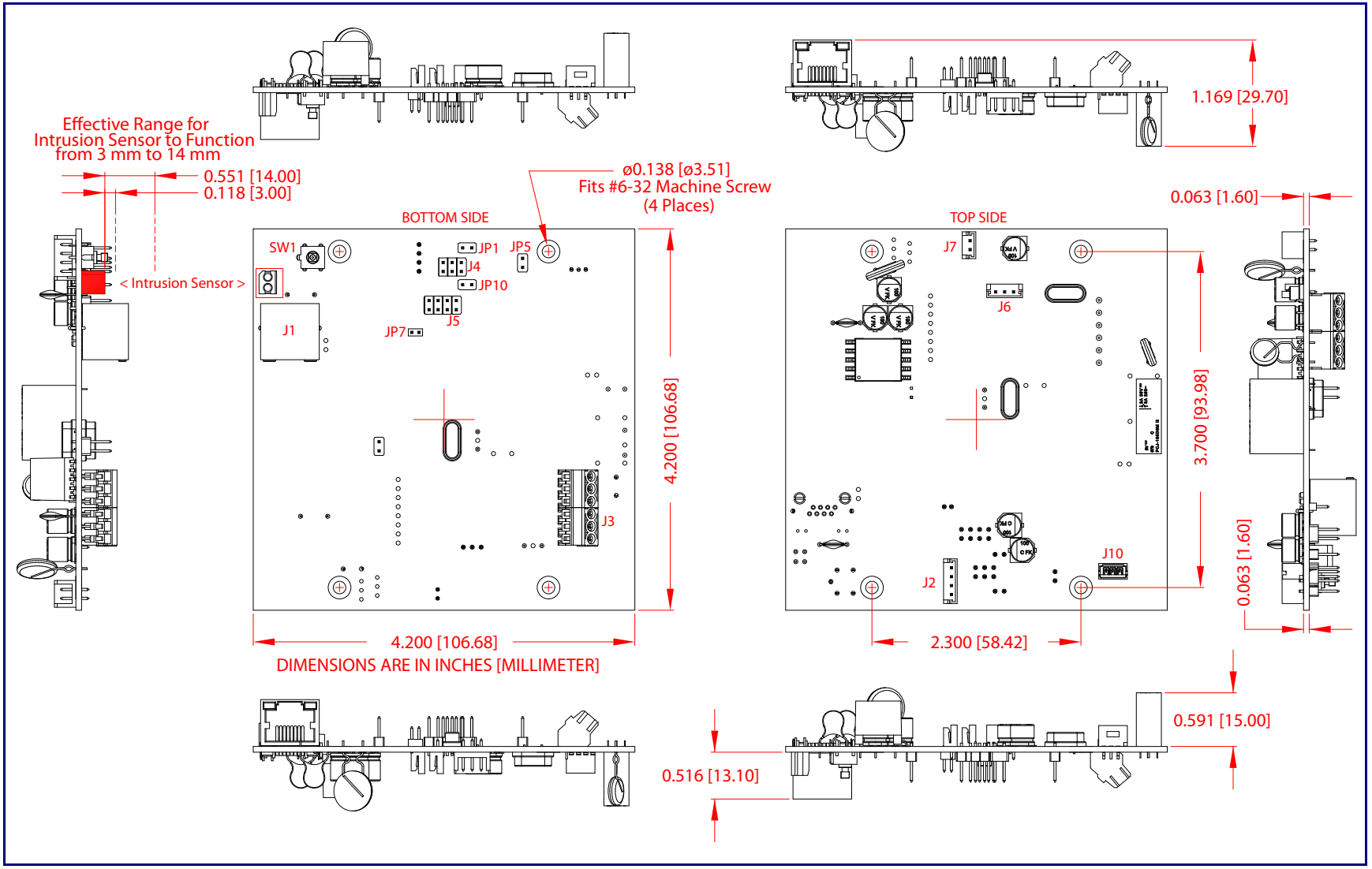


Figure 1-4. PCB Dimensions and Intrusion Sensor Range

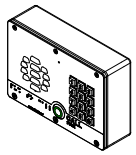
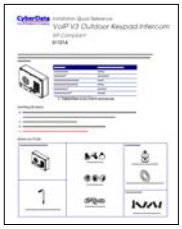


2 Installing the VoIP V3 Outdoor Intercom with Keypad

2.1 Parts List

Table 2-1 illustrates the parts for the VoIP V3 Outdoor Intercom with Keypad.

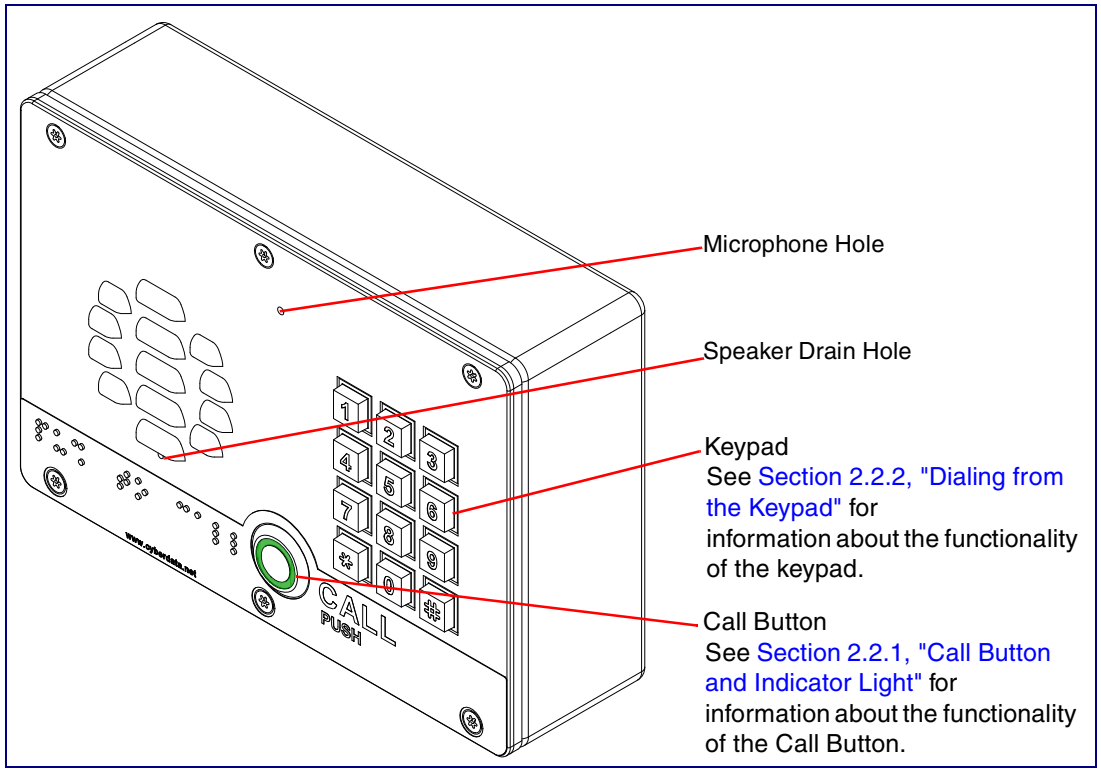
Table 2-1. Parts List

Quantity	Part Name	Illustration
1	VoIP V3 Outdoor Intercom with Keypad Assembly	
1	Installation Quick Reference Guide	
1	Mounting Accessory Kit	

2.2 Intercom Components

Figure 2-1 shows the components of the Intercom .

Figure 2-1. Intercom Components

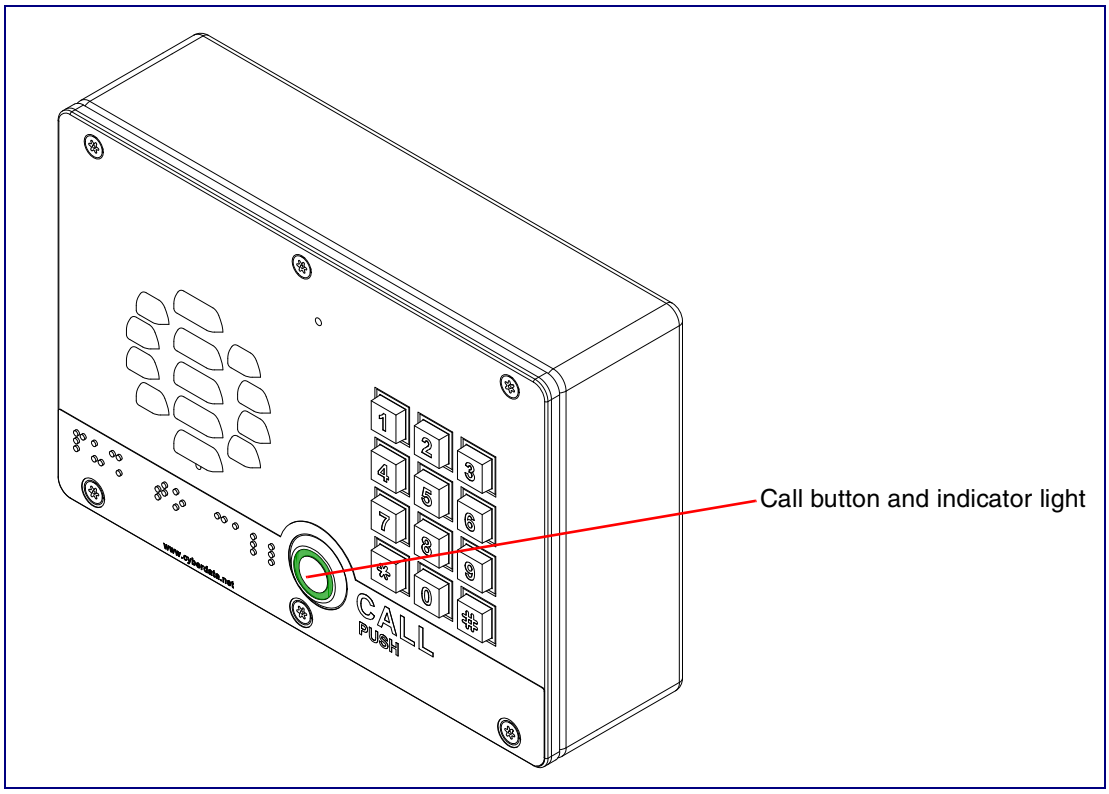

Microphone Hole
Speaker Drain Hole
Keypad
See Section 2.2.2, "Dialing from the Keypad" for information about the functionality of the keypad.
Call Button
See Section 2.2.1, "Call Button and Indicator Light" for information about the functionality of the Call Button.
CALL
PUSH

2.2.1 Call Button and Indicator Light

2.2.1.1 Indicator Light Function

- Upon initial power or reset, the indicator light will illuminate.
- When the software has finished initialization, the indicator light will blink twice.
- When a call is established (not just ringing), the indicator light will blink.
- On the **Device Configuration Page**, there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator light. The indicator light will still blink during initialization and calls.
- The indicator light flashes briefly at the beginning of RTFM mode.

Figure 2-2. Call Button and Indicator Light



2.2.2 Dialing from the Keypad

- See the Enable Telephone Operation setting in Section 2.4.7, "Configure the Button Parameters".

2.3 Intercom Setup

2.3.1 Intercom Connections

Figure 2-3 shows the pin connections on the J3 (terminal block). This terminal block can accept 16 AWG gauge wire.

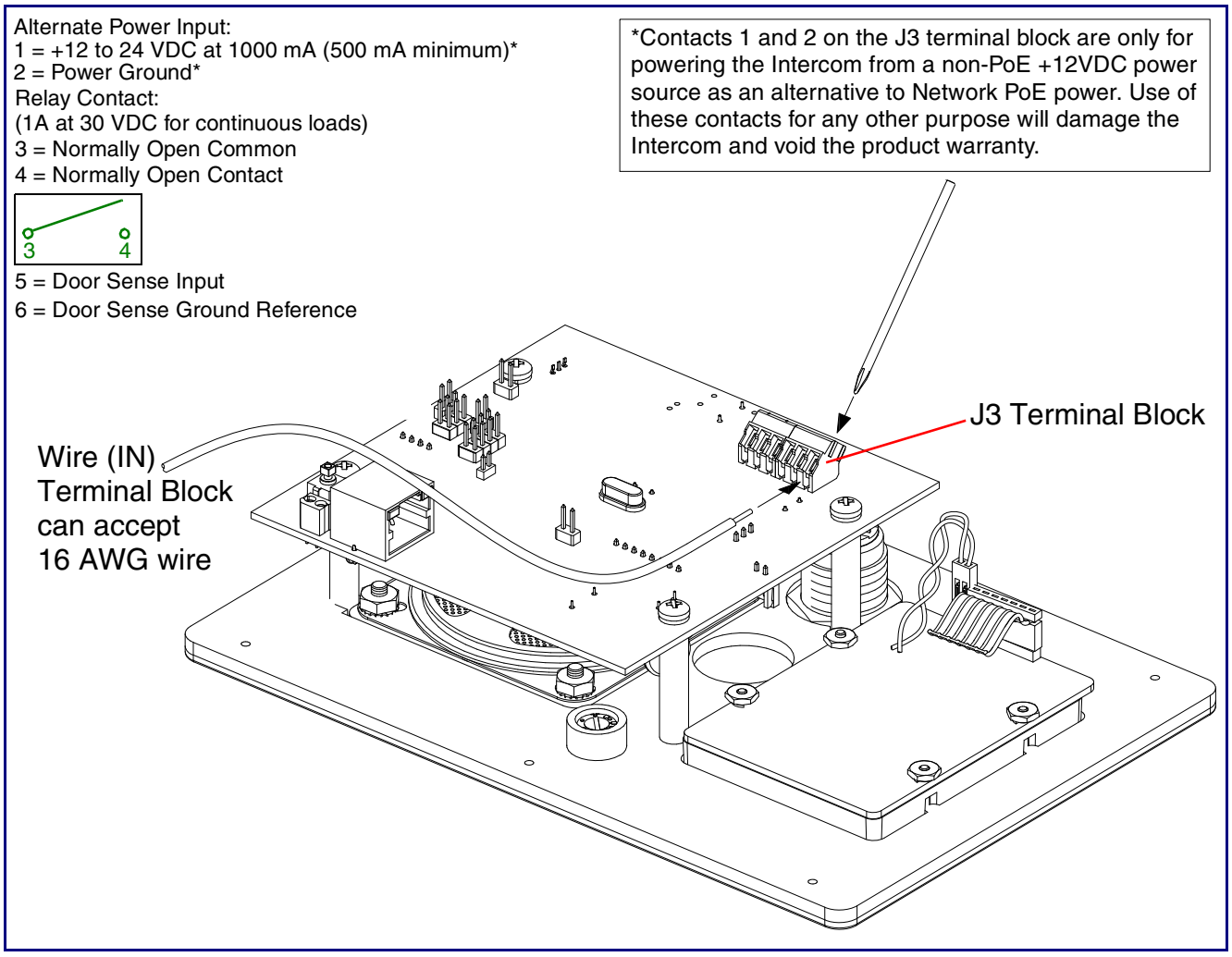
Note As an alternative to using PoE power, you can supply +12 to 24 VDC at 1000 mA (500 mA minimum) into the terminal block.

GENERAL ALERT

Caution

Equipment Hazard: Contacts 1 and 2 on the J3 terminal block are only for powering the Intercom from a non-PoE +12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the Intercom and void the product warranty.

Figure 2-3. Intercom Connections


Alternate Power Input:
1 = +12 to 24 VDC at 1000 mA (500 mA minimum)*
2 = Power Ground*
Relay Contact:
(1A at 30 VDC for continuous loads)
3 = Normally Open Common
4 = Normally Open Contact
3
4
5 = Door Sense Input
6 = Door Sense Ground Reference
*Contacts 1 and 2 on the J3 terminal block are only for powering the Intercom from a non-PoE +12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the Intercom and void the product warranty.
J3 Terminal Block
Wire (IN) Terminal Block can accept 16 AWG wire

2.3.2 Connecting the Intercom to the Auxiliary Relay

Warning

Electrical Hazard: The VoIP Intercom enclosure is not rated for any AC voltages.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Warning

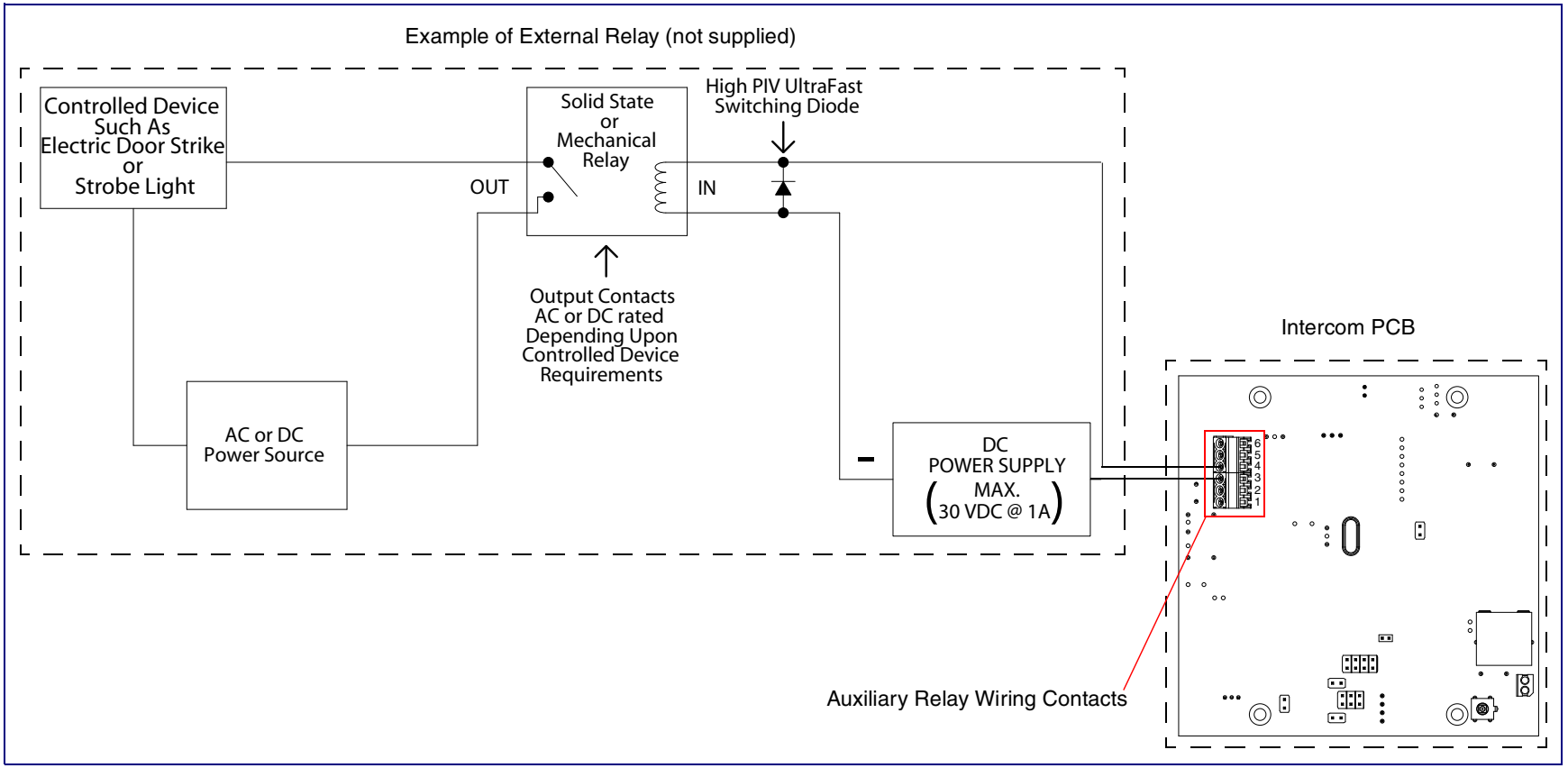
Electrical Hazard: The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

The VoIP Intercom incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see Figure 2-4, "Auxiliary Relay Wiring Diagram").

The Intercom relay contacts are limited to 1A at 30 VDC. The Intercom relay activation time is selectable through the web interface and is controlled by DTMF tones generated from the phone being called. The DTMF tones are selectable from the web interface as well.

Note The three digit code for the auxiliary relay must be sent in conformance with RFC2833 DTMF generation.

Figure 2-4. Auxiliary Relay Wiring Diagram



2.3.3 Identifying the Connector Locations and Functions

See the following figures and tables to identify the board connector locations and functions.

Figure 2-5. Connector Locations

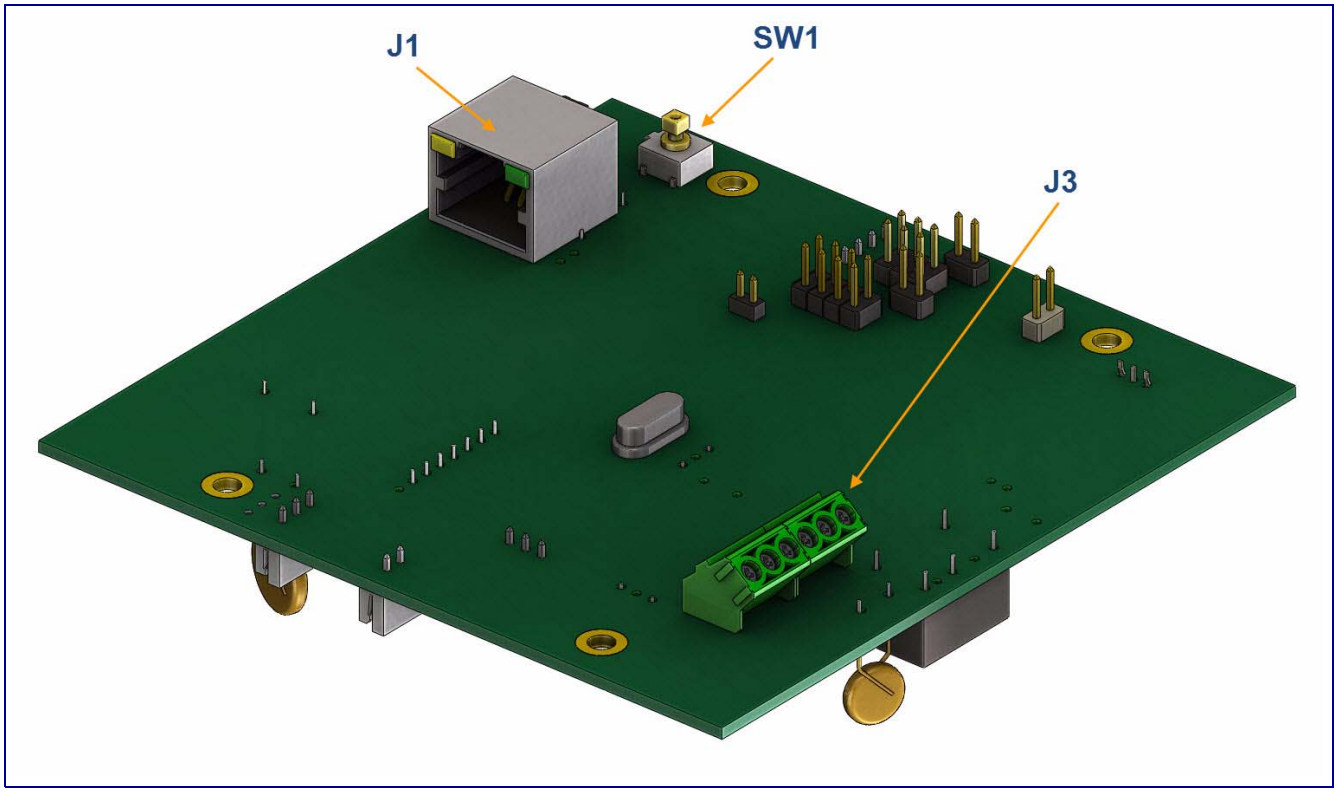


Table 2-2. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J3	Terminal Block (see Figure 2-3)
SW1	RTFM (see Section 2.3.5, "RTFM Button")

Figure 2-6. Connector Locations

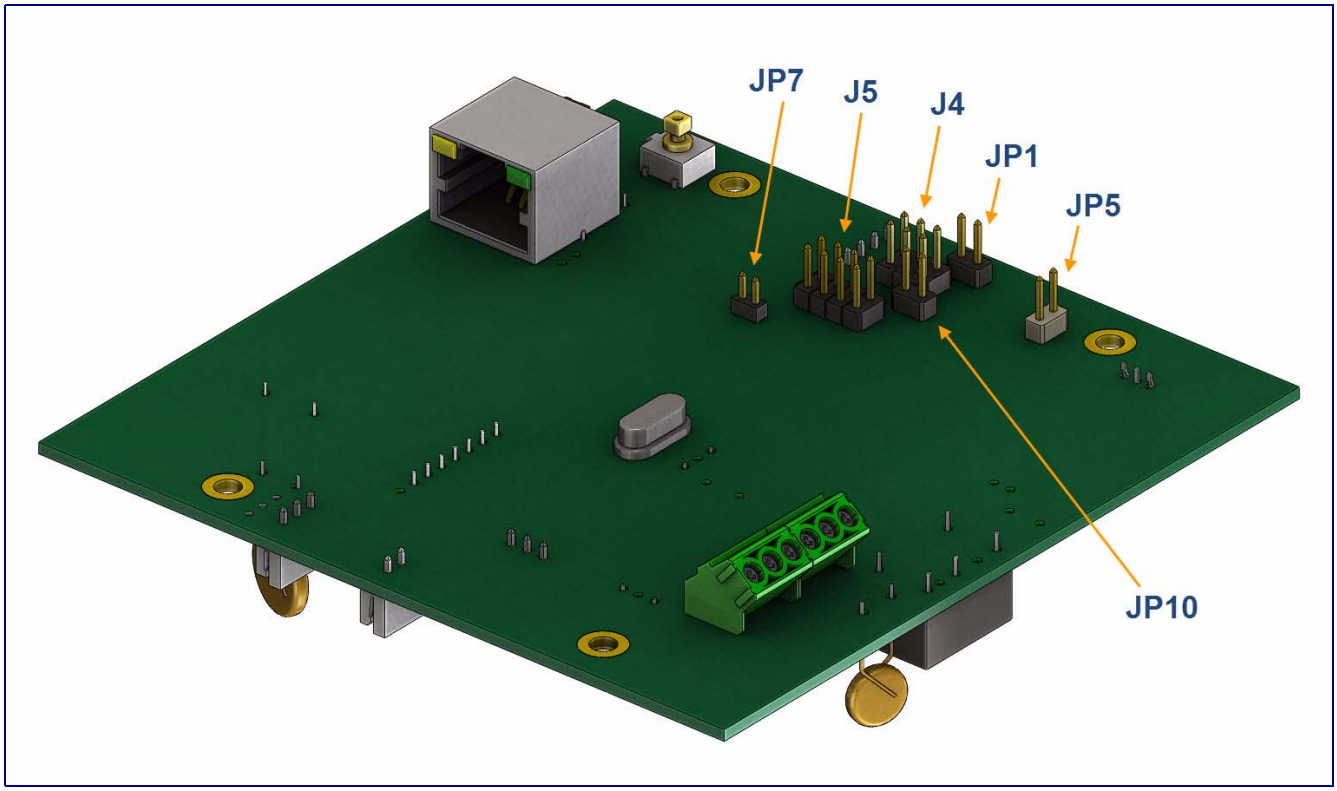


Table 2-3. Connector Functions

Connector	Description	Function
J4	Console	Factory only
J5	J-Tag	Factory only
JP1	Reset	Factory only
JP7	Boot Mode	Factory only
JP5	WD Enable	Not used
JP7	Phy Mode	Not Used
JP10	Intrusion Disable Jumper	Placing a jumper on JP10 will disable the intrusion detection circuit.

Figure 2-7. Connector Locations

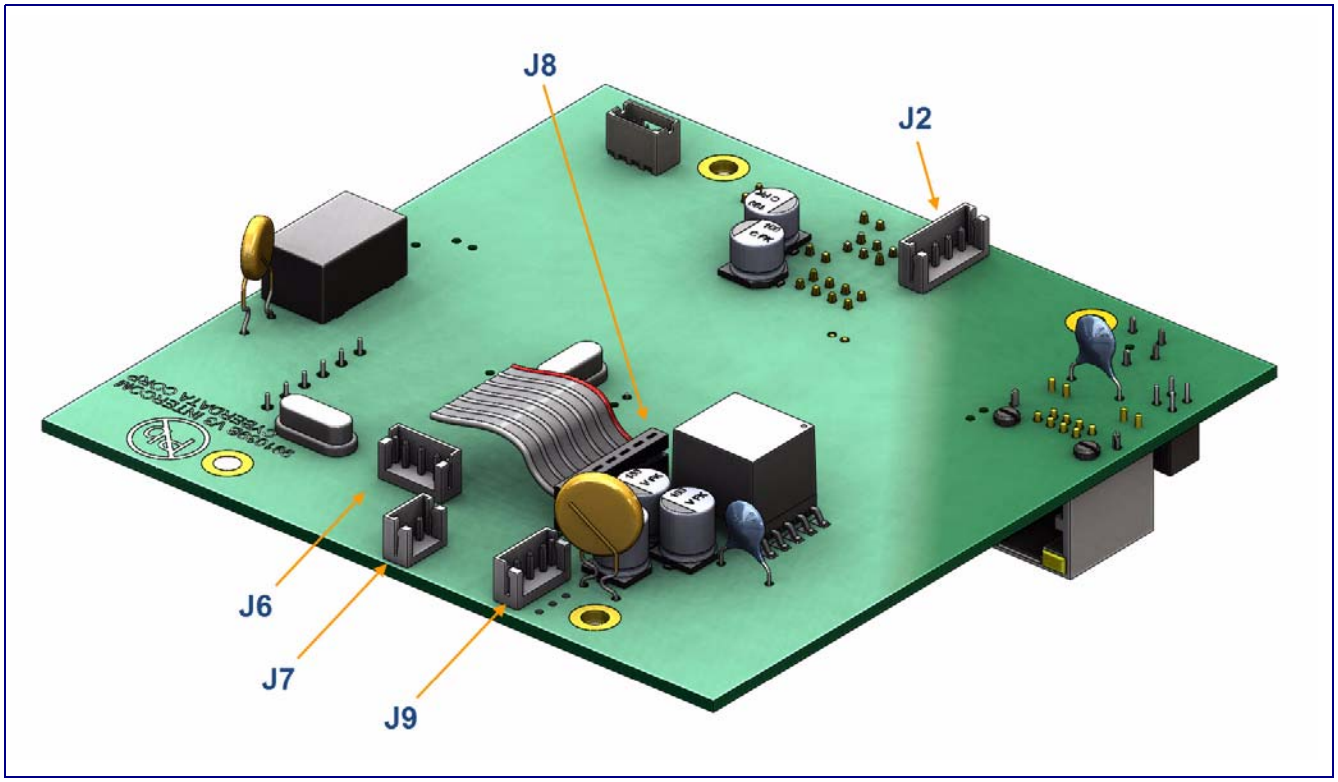


Table 2-4. Connector Functions

Connector	Function
J2	Button/LED Interface
J6	Microphone Interface
J7	Speaker Interface
J8	Keypad Interface
J9	Proximity Sensor Interface

2.3.4 Network Connectivity, and Data Rate

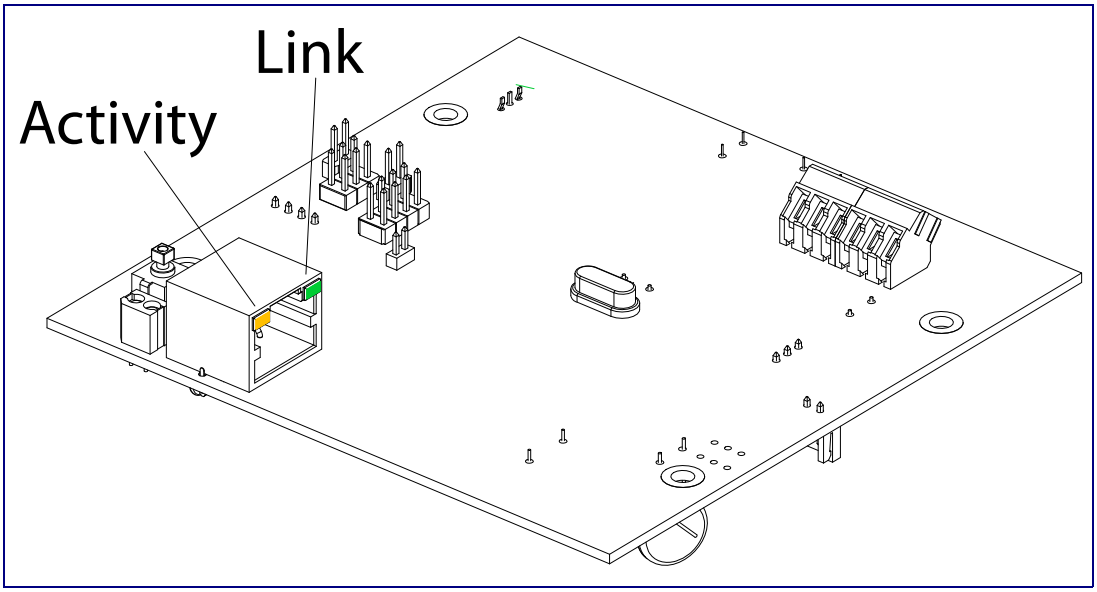
When you plug in the Ethernet cable or power supply:

- The square, green **Link** light above the Ethernet port indicates that the network connection has been established (see Figure 2-8). The Link light changes color to confirm the auto-negotiated baud rate:
  - This light is yellow at 10 Mbps.
  - It is orange at 100 Mbps.

2.3.4.1 Verify Network Activity

The square, yellow **Activity** light blinks when there is network activity.

Figure 2-8. Network Connector

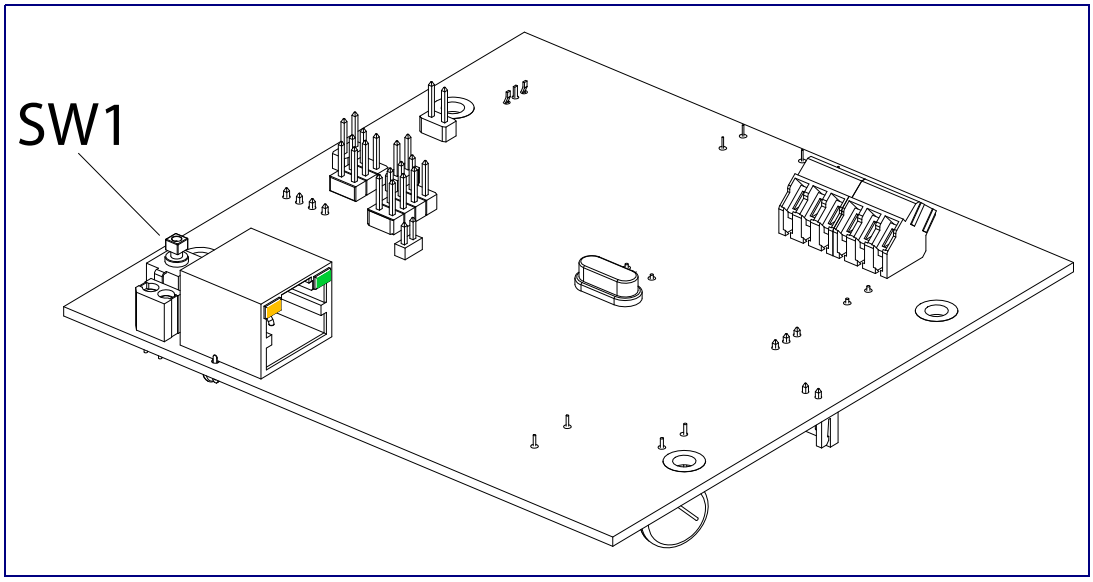


2.3.5 RTFM Button

When the Intercom is operational and linked to the network, use the Reset Test Function Management **(RTFM)** button (see **SW1** in Figure 2-9) on the Intercom board to announce and confirm the Intercom's IP Address and test that the audio is working.

Note You must do this test prior to final assembly.

Figure 2-9. RTFM Button



2.3.5.1 Announcing the IP Address

To announce a device's current IP address:

1. Press and release the RTFM button (SW1) within a five second window.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Note Pressing and holding the RTFM button for longer than five seconds will restore the device to the factory default settings.

2.3.5.2 Restoring the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state.

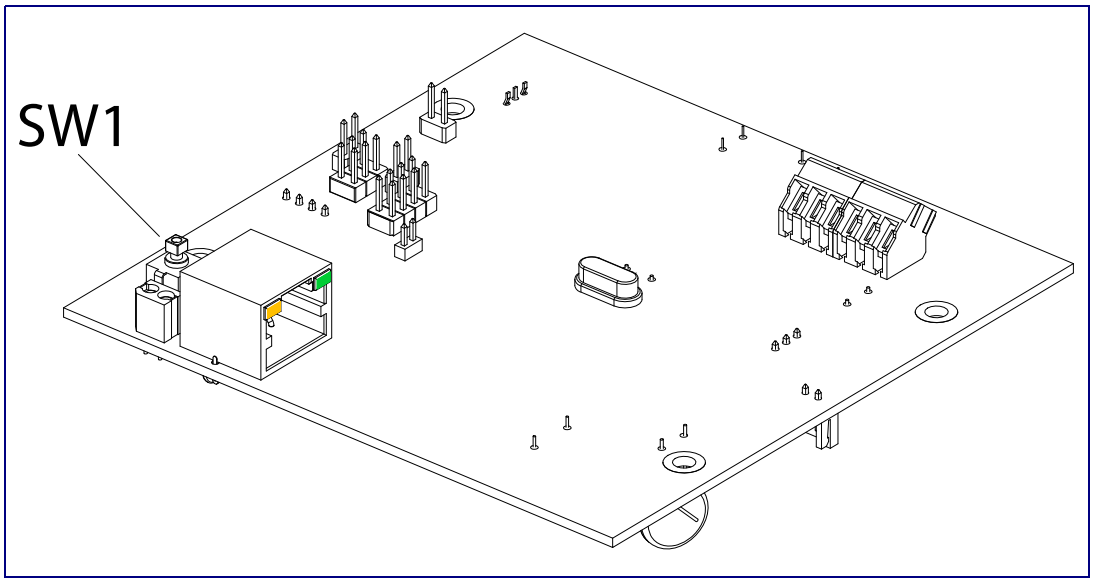
Note Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (SW1) for more than five seconds.
2. The device announces that it is restoring the factory default settings.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Figure 2-10. RTFM Button



2.3.6 Adjust the Volume

You can adjust the volume through the Device Configuration Page.

2.4 Configure the Intercom Parameters

To configure the Intercom online, use a standard web browser.

Configure each Intercom and verify its operation *before* you mount it. When you are ready to mount an Intercom, refer to Appendix A, "Mounting the VoIP V3 Outdoor Intercom with Keypad" for instructions.

2.4.1 Factory Default Settings

All Intercoms are initially configured with the following default IP settings:

When configuring more than one Intercom, attach the Intercoms to the network and configure one at a time to avoid IP address conflicts.

Table 2-5. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

a. Default if there is not a DHCP server present.

2.4.2 Intercom Web Page Navigation

Table 2-6 shows the navigation buttons that you will see on every Intercom web page.

Table 2-6. V2 Paging Amplifier Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device Configuration** page.
	Link to the **Networking** page.
	Link to the **SIP Configuration** page.
	Link to the **Button Configuration** page.
	Link to the **Nightringer Configuration** page.
	Link to the **Sensor Configuration** page.
	Link to the **Multicast Configuration** page.
	Link to the **Audio Configuration** page.
	Link to the **Event Configuration** page.
	Link to the **Autoprovisioning Configuration** page.
	Link to the **Update Firmware** page.

2.4.3 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the Intercom.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

http://www.cyberdata.net/support/voip/discovery_utility.html

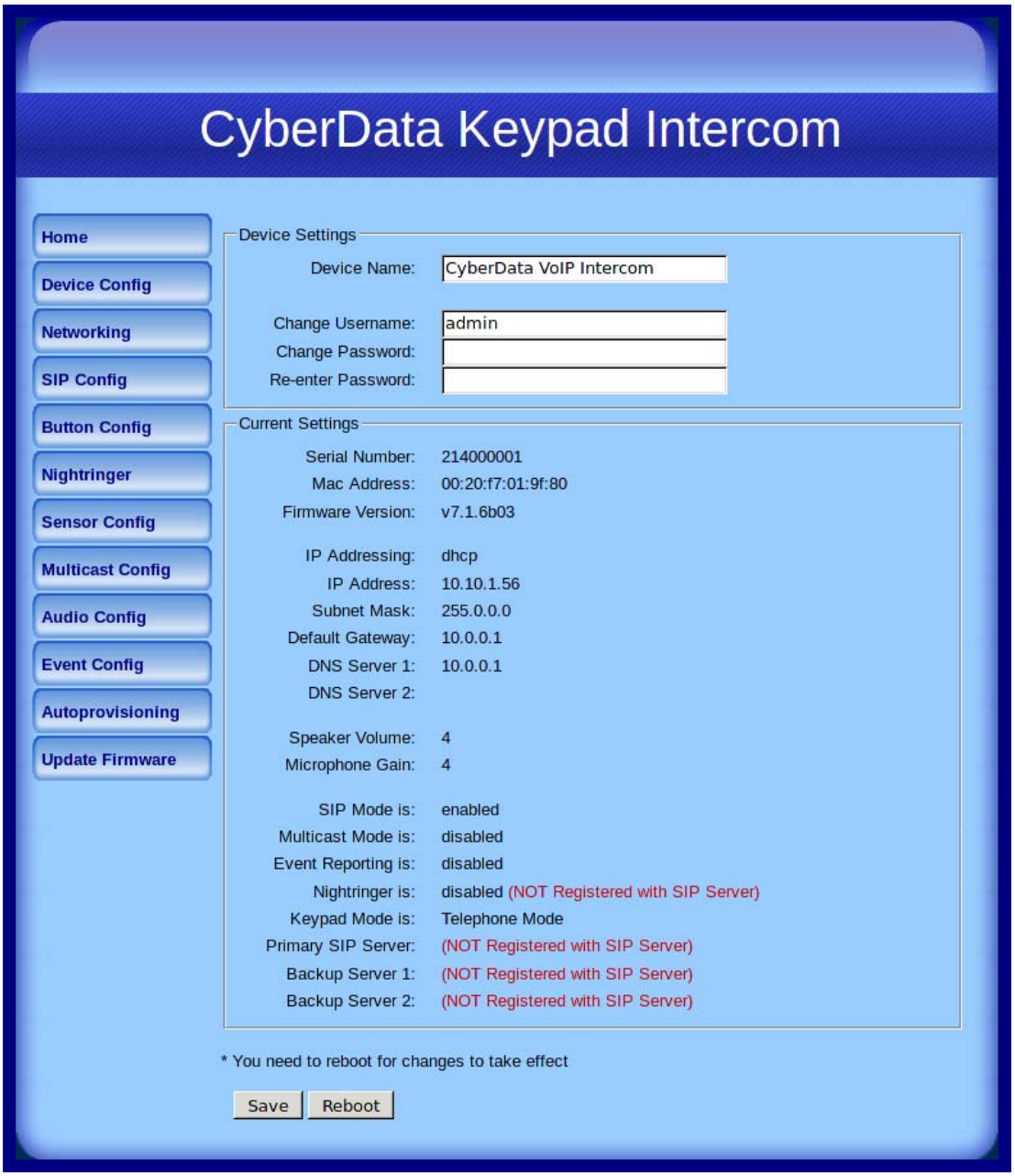
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-11):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-11. Home Page



3. On the **Home Page**, review the setup details and navigation buttons described in Table 2-7.

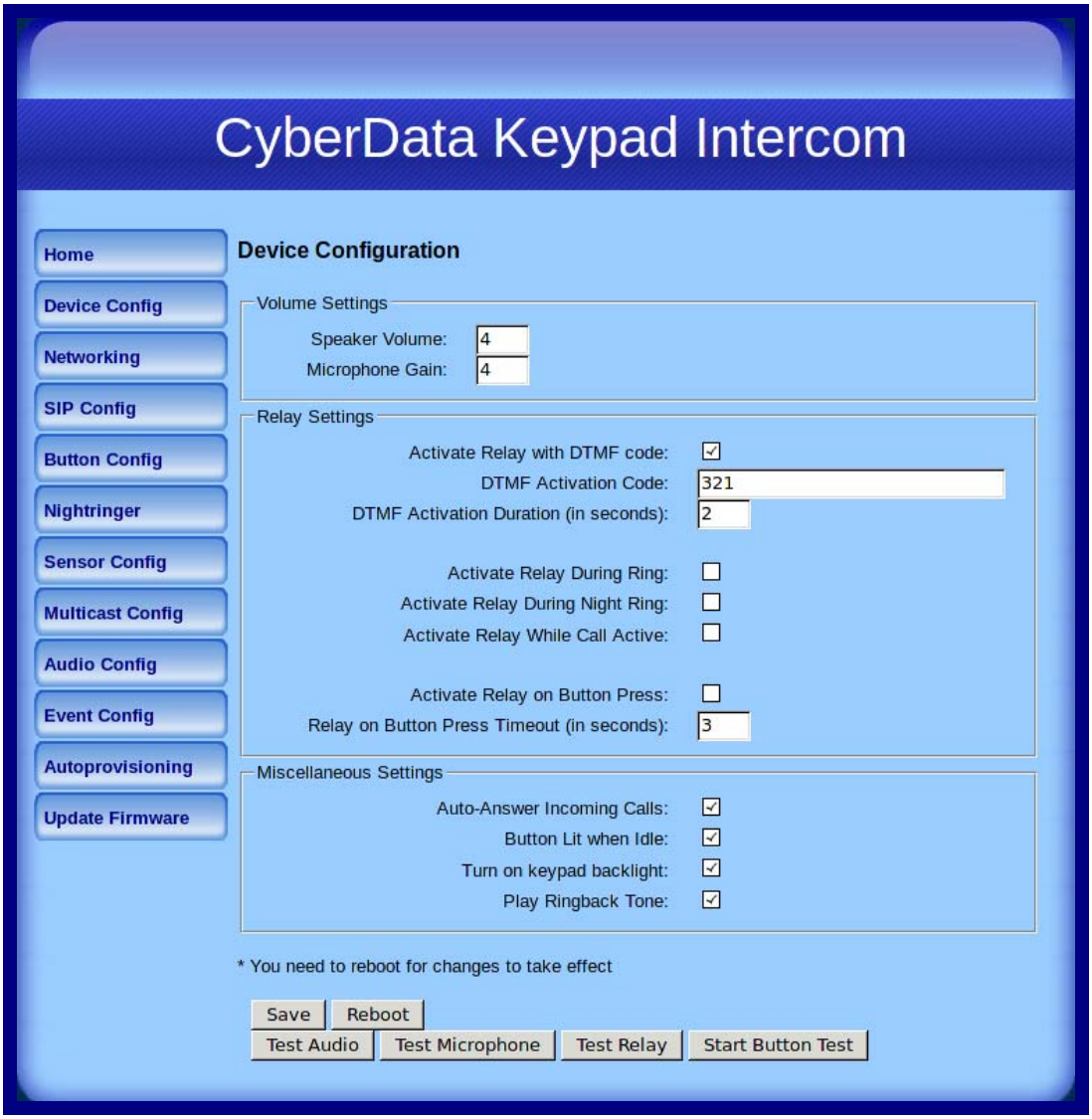
Table 2-7. Home Page Overview

Web Page Item	Description
Device Settings	
Device Name	Shows the device name.
Change Username	Type in this field to change the username.
Change Password	Type in this field to change the password.
Re-enter Password	Type the password again in this field to confirm the new password.
Current Settings	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
Speaker Volume	Shows the current speaker volume level.
Microphone Gain	Shows the current microphone gain level.
SIP Mode is	Shows the current SIP Mode status.
Multicast Mode is	Shows the current Multicast Mode status.
Event Reporting is	Shows the current Event Reporting status.
Nightringer is	Shows the current Nightringer status.
Keypad Mode is	Shows the current Keypad Mode status.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

2.4.4 Configure the Device Parameters

1. Click the **Device Configuration** button to open the **Device Configuration** page. See Figure 2-12.

Figure 2-12. Device Configuration Page



2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 2-8.

Table 2-8. Device Configuration Parameters

Web Page Item	Description
Volume Settings	
Speaker Volume	Type the desired speaker volume level into this field.
Microphone Gain	Type the desired microphone gain level into this field.
Relay Settings	
Activate Relay with DTMF Code	When selected, the relay can be activated with a DTMF code.
DTMF Activation Code	Type the desired DTMF activation code (25 character limit).
DTMF Activation Duration (in seconds)	Type the desired DTMF activation duration (in seconds) (2 character limit [activation times now go up to 99 seconds]). **NOTE**: A DTMF activation duration of **0** will toggle the relay indefinitely or until the activation code is sent again
Activate Relay During Ring	When selected, the relay will be activated for as long as the call is active. **NOTE**: When the phone is set to **Auto Answer**, it will not ring and this option does nothing.
Activate Relay During Night Ring	Check this box to activate the relay for as long as a Night Ring tone is ringing.
Activate Relay While Call Active	When selected, the relay will be activated for as long as the call is active.
Activate Relay on Button Press	When selected, the relay will be activated when the Call Button is pressed.
Relay on Button Press Timeout (in seconds)	Type the desired time (in seconds) that you want the relay to activate after the Call Button is pressed (1 character limit).
Miscellaneous Settings	
Auto-Answer Incoming Calls	When selected, the device will automatically answer incoming calls. When **Auto Answer** is Off, the device will play a ringtone through the Intercom speaker until someone presses the button.
Button Lit When Idle	When selected, the Call Button remains lit when idle.
Turn on keypad backlight	When selected, the keypad backlight will be turned on.
Play Ringback Tone	When selected, you will hear a ringback tone while making a call.
	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.

Table 2-8. Device Configuration Parameters (continued)

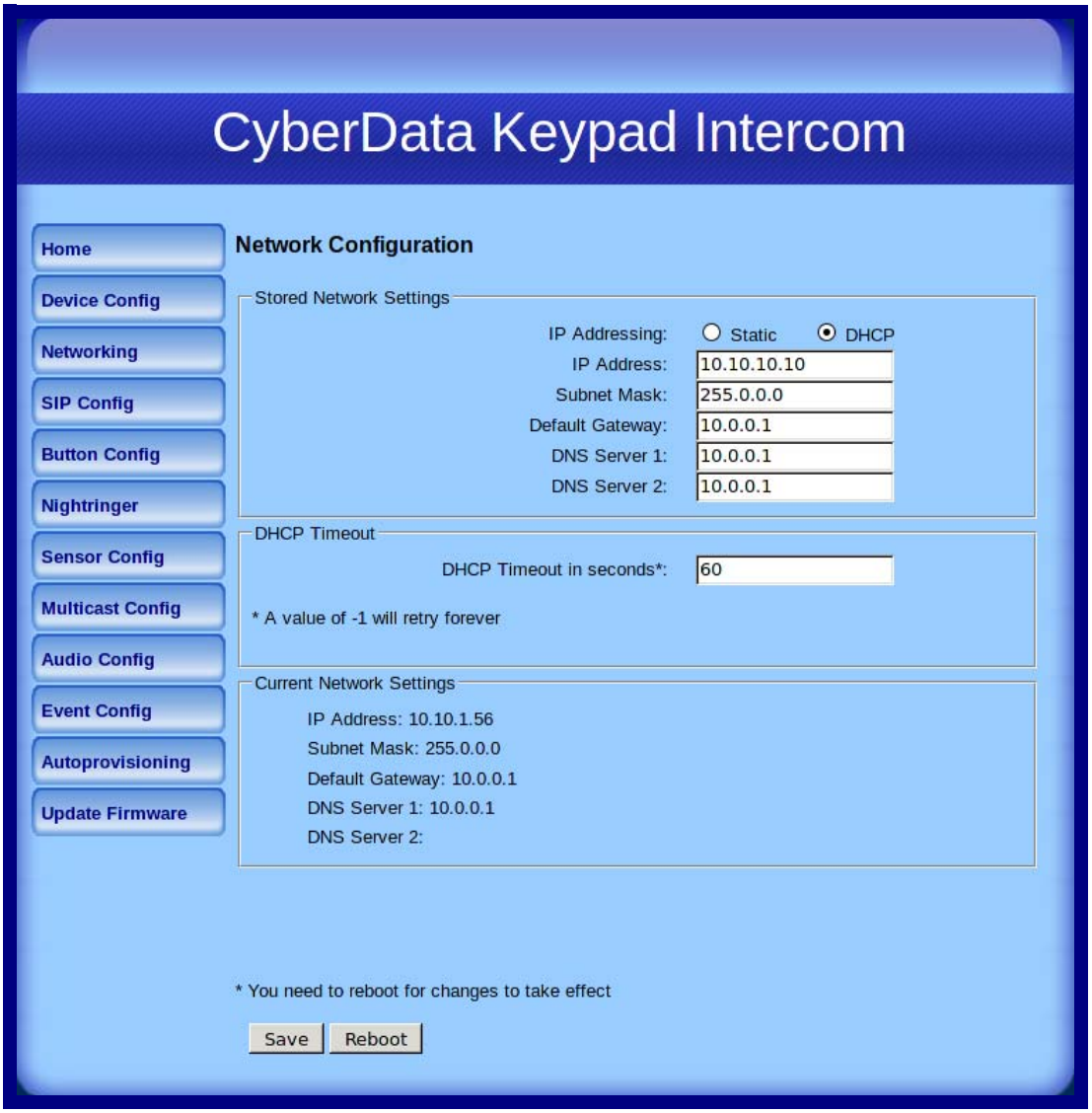
Web Page Item	Description
Test Microphone	Click on the **Test Microphone** button to do a microphone test. When the **Test Microphone** button is pressed, the following occurs: 1. The device will immediately start recording 3 seconds of audio. 2. The device will beep (indicating the end of recording). 3. The device will play back the recorded audio.
Test Relay	Click on the **Test Relay** button to do a relay test.
Start Button Test	Click on the **Test Relay** button to do a button test. When pressed, the button text will change to **Stop Button Test** and in this mode, pressing the button will play test audio. Also, pressing this button also puts the device into a mode where it will play audio as the buttons are pressed. For buttons 0-9 it will play the audio file for that number. For buttons '*', '#', and the Call Button, it will play the appropriate DTMF tones.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.4.5 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-13).

Figure 2-13. Network Configuration Page



2. On the **Network Configuration** page, enter values for the parameters indicated in Table 2-9.

Table 2-9. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	Shows the settings stored in non-volatile memory.
IP Addressing	Select either **DHCP IP Addressing** or **Static IP Addressing** by marking the appropriate radio button. If you select **Static**, configure the remaining parameters indicated in Table 2-9. If you select **DHCP**, go to Step 3.
IP Address	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1	Enter the DNS Server 1 address.
DNS Server 2	Enter the DNS Server 2 address.
DHCP Timeout	
DHCP Timeout in seconds	Enter the desired timeout duration (in seconds) that the device will wait for a response from the DHCP server before defaulting back to the stored static IP address. **Note**: A value of **-1** will cause the device to retry indefinitely and a value of **0** will cause the device to reset to a default of 60 seconds.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**. This updates the changed parameters and reboots the Intercom if appropriate.

4. Connect the Intercom to the target network.

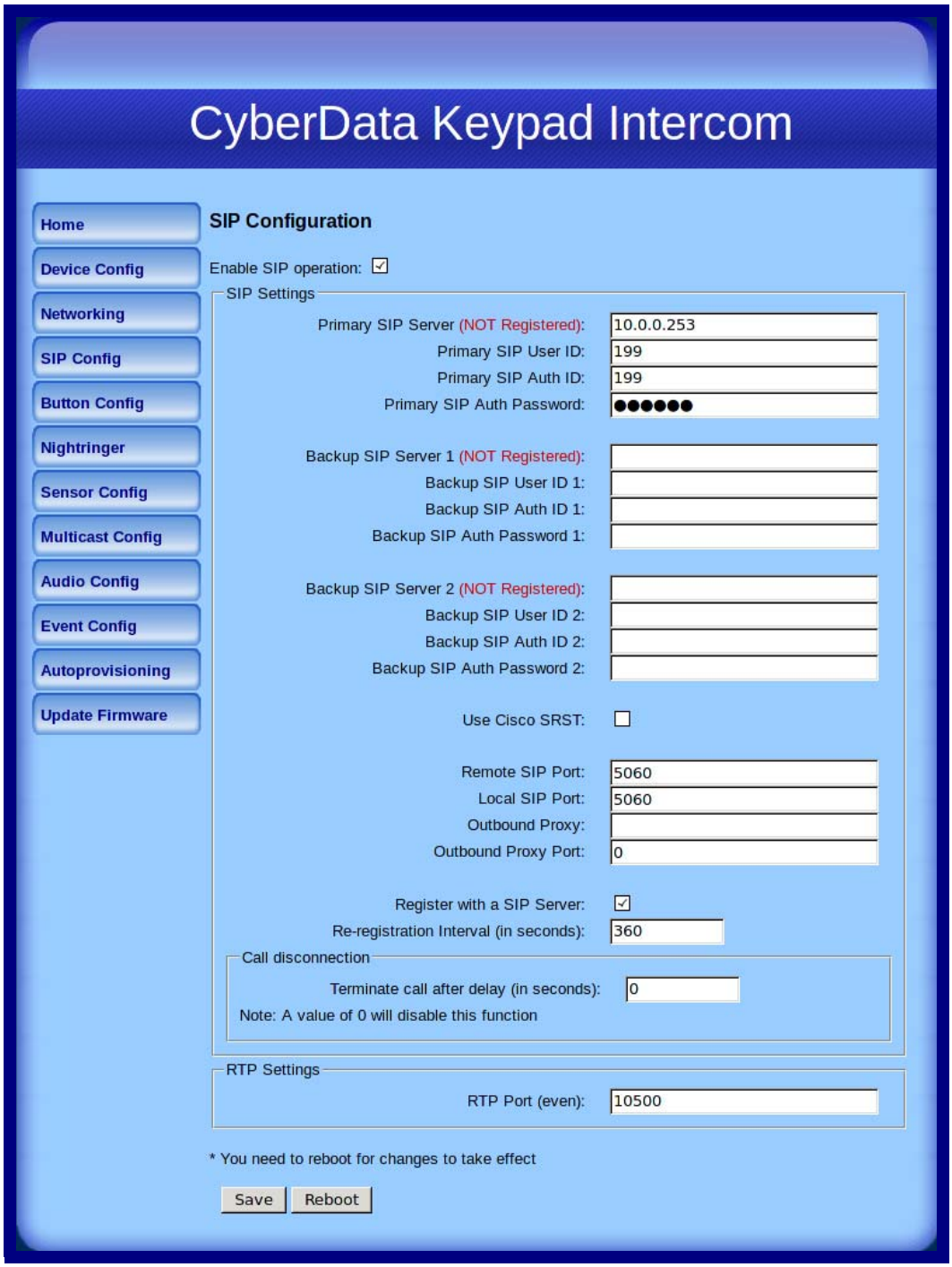
5. From a system on the same network as the Intercom, open a browser with the new IP address of the Intercom.

2.4.6 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-14).

Note For specific server configurations, go to the following website address:
http://www.cyberdata.net/support/server/index.html

Figure 2-14. SIP Configuration Page



2. On the **SIP Configuration** page, enter values for the parameters indicated in Table 2-10.

Table 2-10. SIP Configuration Parameters

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
SIP Settings	
Primary SIP Server	Use this field to set the address (in dotted decimal notation or as a canonical name) for the Primary SIP Server. This field can accept canonical names of up to 255 characters in length.
Primary SIP User ID	Type the **SIP User ID** for the Primary SIP Server (up to 64 alphanumeric characters).
Primary Auth ID	Type the **Authenticate ID** for the Primary SIP Server (up to 64 alphanumeric characters).
Primary SIP Auth Password	Type the **Authenticate Password** for the Primary SIP Server (up to 64 alphanumeric characters).
Backup SIP Server 1 Backup SIP Server 2	• If all of the **Primary SIP Server** and **Backup SIP Server** fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the **Backup SIP Server 1** and **Backup SIP Server 2** fields blank if they are not needed. • In the event of a registration failure on the **Primary SIP Server**, the device will use the next highest priority server for outbound calls (**Backup SIP Server 1**). If **Backup SIP Server 1** fails, the device will use **Backup SIP Server 2**. • If a higher priority SIP Server comes back online, the device will switch back to this server.
Backup SIP User ID 1 Backup SIP User ID 2	Type the **SIP User ID** for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth ID 1 Backup SIP Auth ID 2	Type the **SIP Authenticate ID** for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth Password 1 Backup SIP Auth Password 2	Type the **SIP Authenticate Password** for the Backup SIP Server (up to 64 alphanumeric characters).
Use Cisco SRST	When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).
Remote SIP Port*	Type the **Remote SIP Port** number (default 5060) (8 character limit).
Local SIP Port*	Type the **Local SIP Port** number (default 5060) (8 character limit).
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (8 character limit).
Register with a SIP Server*	Check this box to enable SIP Registration. For information about Point-to-Point Configuration, see Section 2.4.6.1, "Point-to-Point Configuration".

Table 2-10. SIP Configuration Parameters (continued)

Web Page Item	Description
Re-registration Interval (in seconds)*	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)*
Call Disconnection	
Terminate call after delay (in seconds)	Type the desired number of seconds that you want to transpire before a call is terminated. Note: A value of **0** will disable this function.
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

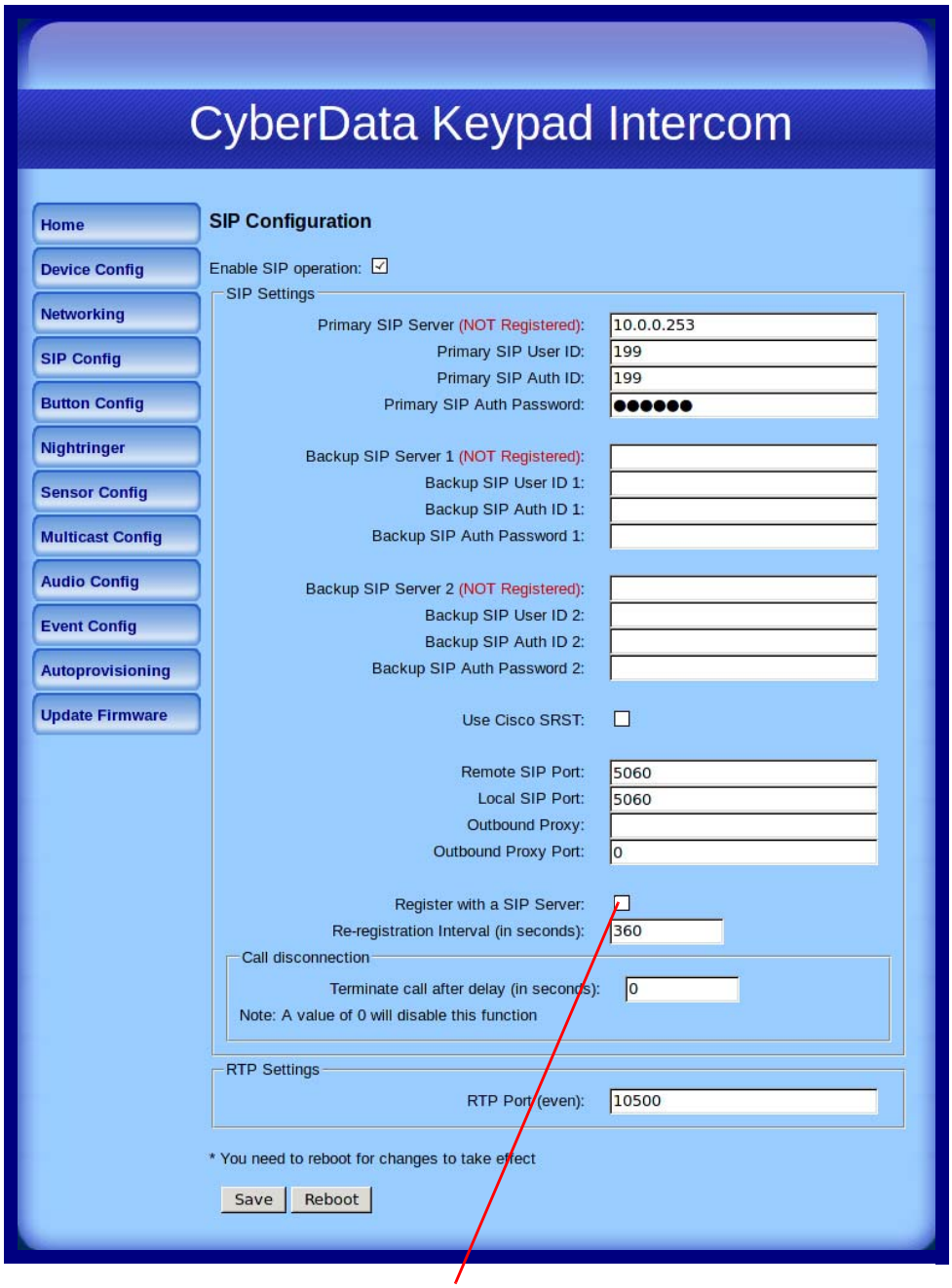
3. After changing the parameters, click **Save Settings**.

2.4.6.1 Point-to-Point Configuration

When the board is set to not register with a SIP server, it's possible to set the device to dial out to a single endpoint. To do this, do the following:

1. On the **SIP Configuration** page (Figure 2-15), make sure that the **Register with a SIP Server** parameter is not selected.

Figure 2-15. SIP Configuration Page Set to Point-to-Point Mode



2. On the **Button Configuration** page (Figure 2-16 and Figure 2-17), type the IP address of the remote device that you want to contact into a **Keypad** or **Call Button** field (in either **Speed Dial Mode** or **Security Dial Mode**).

Note There is no way to place a point-to-point call in **Telephone Dial Mode** or **Cellphone Dial Mode**. The Intercom can receive point-to-point calls in any mode.

Note The delayed DTMF functionality is available in the Point-to-Point Mode.

Note Establishing point-to-point SiP calls may not work with all phones.

2.4.7 Configure the Button Parameters

1. Click the **Button Config** button to open the **Button Configuration** page. See Figure 2-16.

Figure 2-16. Button Configuration Page

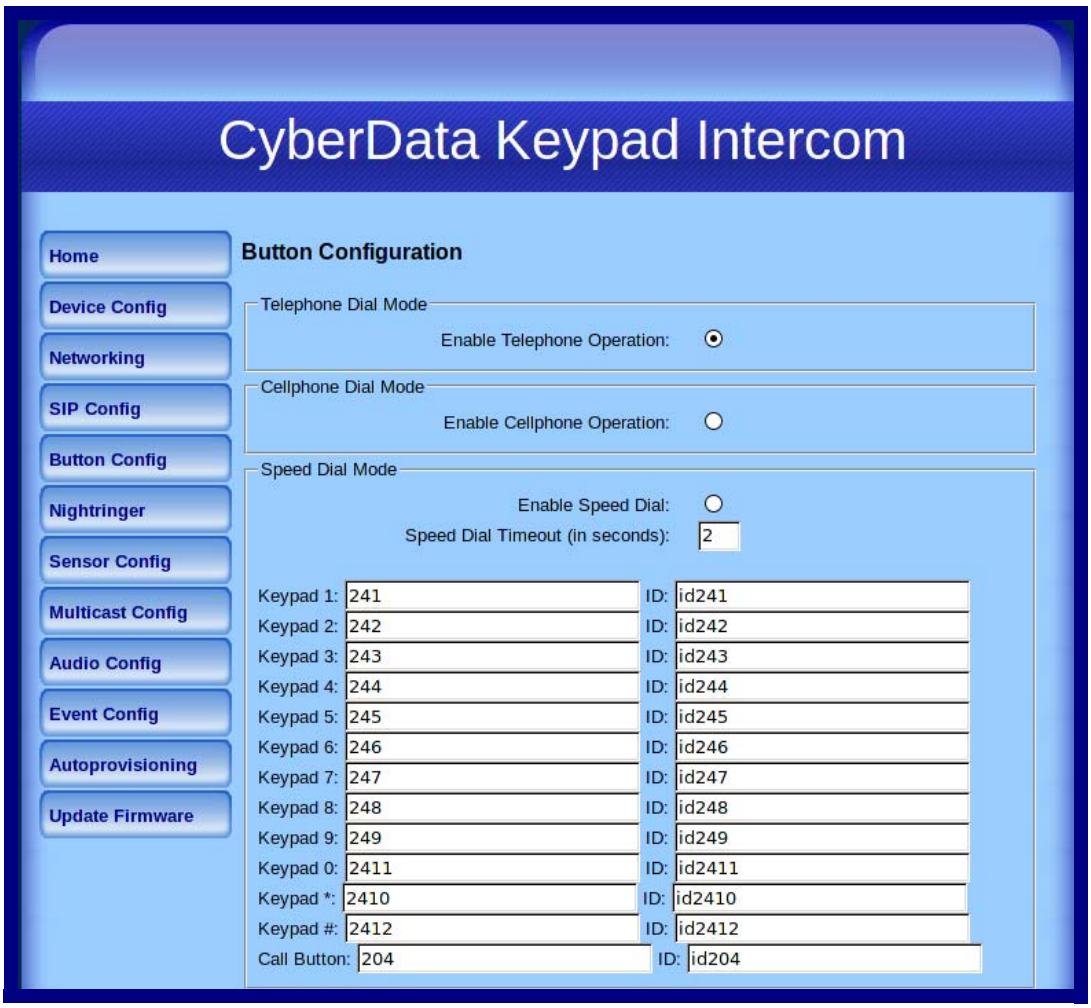
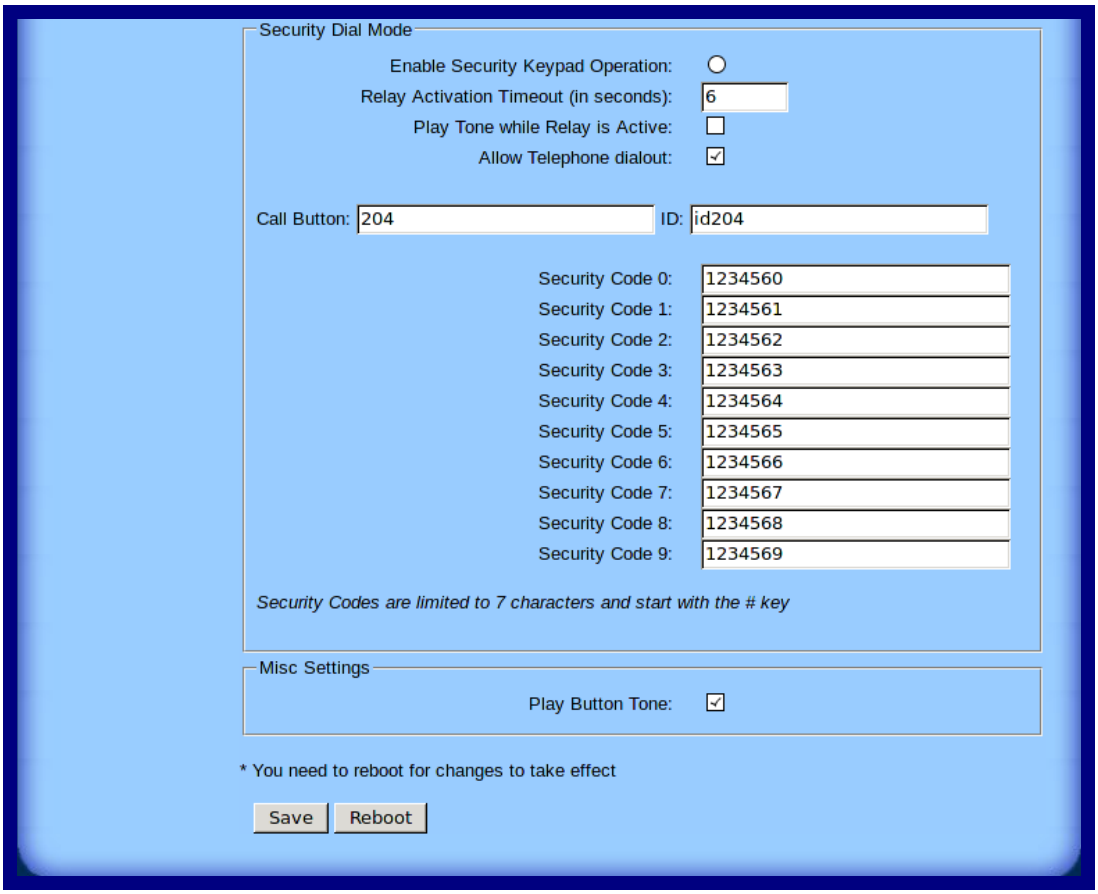


Figure 2-17. Button Configuration Page (continued)


Security Dial Mode
Enable Security Keypad Operation:
Relay Activation Timeout (in seconds): 6
Play Tone while Relay is Active:
Allow Telephone dialout:
Call Button: 204
ID: id204
Security Code 0: 1234560
Security Code 1: 1234561
Security Code 2: 1234562
Security Code 3: 1234563
Security Code 4: 1234564
Security Code 5: 1234565
Security Code 6: 1234566
Security Code 7: 1234567
Security Code 8: 1234568
Security Code 9: 1234569
Security Codes are limited to 7 characters and start with the # key
Misc Settings
Play Button Tone:
* You need to reboot for changes to take effect
Save
Reboot

2. On the **Button Configuration** page, you may enter values for the parameters indicated in Table 2-11.

Table 2-11. Button Configuration Parameters

Web Page Item	Description
Telephone Dial Mode	
Enable Telephone Operation	Select **Enable Telephone Operation** to put the Intercom into **Telephone Dial Mode**. In **Telephone Dial Mode**, the Intercom will operate like a telephone: • To make a call in this mode, press the Call Button to go 'off-hook'. The unit will begin playing a dial tone and will wait for keypad input. • Dial the extension you want to reach and wait. • Pressing the Call Button at any time in this process will hang up the call (put it back 'on-hook'). • During a call, you can use the keypad to send DTMF tones to the remote extension.
Cellphone Dial Mode	
Enable Cellphone Operation	Select **Enable Cellphone Operation** to put the Intercom into **Cellphone Dial Mode**. In **Cellphone Dial Mode**, the Intercom will operate like a cellular phone: • This mode is similar to the telephone operation but you dial in an extension differently. • To make a call in this mode, dial the extension and then press the call button to 'send' or initiate the call. • Pressing the call button at any time in this process will hang up the call (put it back 'on-hook'). • During a call you can use the keypad to send DTMF tones to the remote extension.
Speed Dial Mode	
Enable Speed Dial	Select **Enable Speed Dial** to put the Intercom into **Speed Dial Mode**. In this mode the user sets up extensions to dial when a button is pressed. The **Speed Dial Timeout (in seconds)** setting is the number of seconds you need to hold the button before it will place a call. If this value is **0**, it will place a call as soon as the button is released. The speed dial fields in this mode will accept delayed DTMF tones when a comma ',' is in the dial-out field.
Speed Dial Timeout (in seconds)	Type the desired time (in seconds) that you want a button held before it will initiate a call. **Note**: A **Speed Dial Timeout** setting of **0** will start a call as soon as the button is released.
Keypad (0 through 9, *, and #)	Enter the desired dial-out extension number (64 character limit). **Note**: For information about dial-out extension strings and DTMF tones, see Section 2.4.7.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".

Table 2-11. Button Configuration Parameters (continued)

Web Page Item	Description
Call Button	Enter the desired dial-out extension number (64 character limit). **Note**: For information about dial-out extension strings and DTMF tones, see Section 2.4.7.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".
Security Dial Mode	
Enable Security Keypad Operation	Select **Enable Security Keypad Operation** to put the Intercom into **Security Dial Mode**. In **Security Dial Mode**, the Intercom will act like a normal, one-button Intercom by calling the extension specified in the **Call Button** field. When a security code is entered on the keypad that matches one of the seven-digit fields specified on the page, the relay will be activated. • This mode is meant for installation with security doors. In **Security Dial Mode**, the Intercom will act like a normal, one-button Intercom by calling the extension specified in the **Call Button** field. • Up to 10 (7-digit maximum) security codes can be registered with the device. Enter a security code by pressing the **#** key before entering the code. When one of these codes is typed on the keypad, it will activate the relay for the **Relay Activation Timeout (in seconds)** setting. • It is possible to enter a security code both inside and out of calls. • In this mode normal relay operation is suspended and the following settings are non-operational: **Relay On Button Press,** **Relay During Call Active** **Relay During Ring** **Relay During Night-ring** • In this mode, you can't send dtmf to a remote extension using the keypad. You can however setup delayed dtmf tones in the dial out string.
Relay Activation Timeout (in seconds)	Type the desired length of time (in seconds) that you want the relay to remain activated after a security code is entered.
Play Tone While Relay is Active	Check this box to play an audible tone while the relay is activated.

Table 2-11. Button Configuration Parameters (continued)

Web Page Item	Description
Allow Telephone Dialout	When the **Allow Telephone Dialout** option is enabled, you can use the keypad to place calls to a dialed extension. To call an extension, dial the number and wait. You can still enter security codes with the **Allow Telephone Dialout** option enabled by pressing the **#** key before entering the code. With the **Allow Telephone Dialout** option disabled, all keypad input will be treated as security input. You can still use the # key but it is not necessary. For information about how to instantly triggering a dialout call or security code, see Section 2.4.7.2, "Triggering a Dialout Call or Security Code".
Call Button	Enter the desired dial-out extension number (64 character limit). Security codes are limited to seven characters and are activated with the # key. **Note**: For information about dial-out extension strings and DTMF tones, see Section 2.4.7.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".
ID	Type the desired Extension ID (64 character limit).
Security Code (0 through 9)	Enter the desired security code number (7 character limit). When a security code is entered on the keypad that matches one of the seven-digit fields specified on the page, the relay will be activated.
Misc Settings	
Play Button Tone	Check this box to hear a tone when a keypad button is pushed. This setting applies to all modes and determines whether the device will play an audible sound out of the speaker when doing any of the following: • Entering a security code • Initiating a speed dial • Pressing the keys in cellphone and telephone modes
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.4.7.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

On the **Button Configuration** page, dial out extensions support the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-12. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 25.

2.4.7.2 Triggering a Dialout Call or Security Code

You can instantly trigger a dialout call or security code by pressing the **#** key after dialing a number. Table 2-13 shows the various actions that result from different keypad input.

Table 2-13. Triggering a Dialout Call or Security Code

Allow Telephone Dialout Option Enabled (in security mode with default security settings)	
Input	**Resulting Action**
Dialing **123** (and waiting for several seconds)	The device will call extension **123** through the default SIP server.
Dialing **#123** (and waiting for several seconds)	The device will do nothing. The entry is an unrecognized security entry.
Dialing **#1234560** (and waiting for several seconds)	The device will activate the relay for **Security Code 0** for **6** seconds.
Dialing **#124560#**	The device will instantly activate the relay for **6** seconds.
Dialing **123#**	The device will instantly call extension **123** through the default SIP server.
Allow Telephone Dialout Option Disabled (in security mode with default security settings)	
Input	**Resulting Action**
Dialing **1234560** (and waiting for several seconds)	The device will activate the relay for **Security Code 0** for **6** seconds.

2.4.8 Configure the Night Ringer Parameters

When the Nightringer is enabled, the Intercom will register as a second SIP extension. Registration does not have to be to the same server as the primary SIP registration. Any calls made to the Nightringer extension will cause the Intercom to play a ring tone. There is no way to answer this call. The Nightringer is designed to be used in buildings where calls made after hours are directed to a ring group.

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See Figure 2-18.

Figure 2-18. Nightringer Configuration Setup

2. On the **Nightringer Configuration** page, enter values for the parameters indicated in Table 2-14.

Table 2-14. Nightringer Configuration Parameters

Web Page Item	Description
Enable Nightringer	When the nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone.
Nightringer Settings	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation.
Remote SIP Port	Type the Remote SIP Port number (default 5060) (8 character limit).
Local SIP Port	Type the Local SIP Port number (default 5060) (8 character limit). **Note**: This value cannot be the same as the **Local SIP Port*** found on the **SIP Configuration Page**.
User ID	Type the **User ID** (up to 64 alphanumeric characters).
Authenticate ID	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)*	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)*
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.4.9 Configure the Sensor Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor Configuration** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

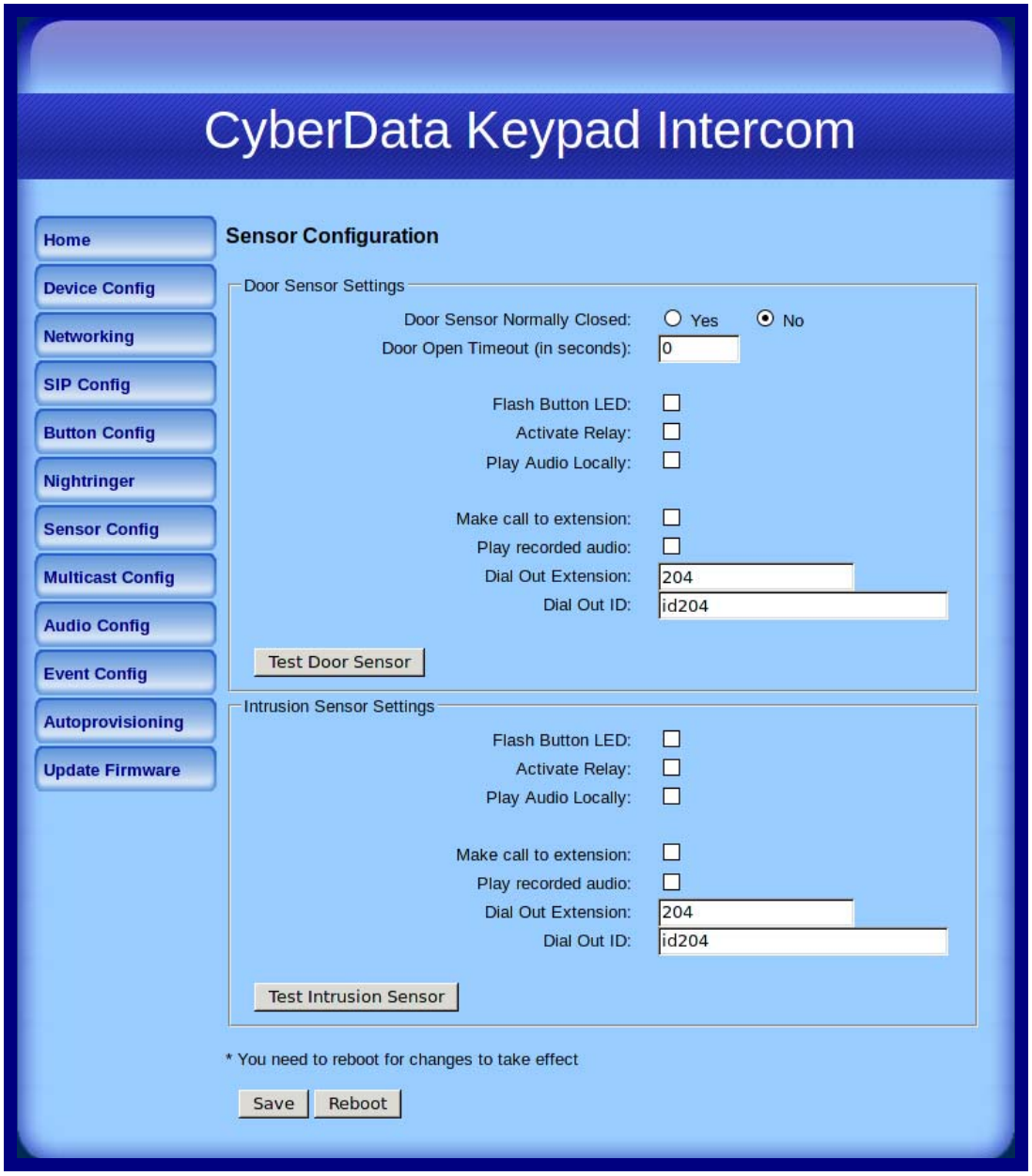
For each sensor there are four actions the Intercom can take:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the Intercom speaker until the sensor is deactivated
- Call a preset extension and play a pre-recorded audio file (once)

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

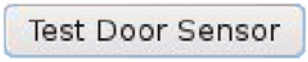
1. Click **Sensor Config** to open the **Sensor Configuration** page (Figure 2-19).

Figure 2-19. Sensor Configuration Page



2. On the **Sensor Configuration** page, enter values for the parameters indicated in Table 2-15.

Table 2-15. Sensor Configuration Parameters

Web Page Item	Description
Door Sensor Settings	
Door Sensor Normally Closed	Select the inactive state of the door sensors.
Door Open Timeout (in seconds)	Select the number of seconds that you want to pass before the door sensor is activated.
Flash Button LED*	Check this box to flash the LED until the sensor is deactivated (roughly 10 times/second).
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Play Audio Locally	Check this box to loop an audio file out of the Intercom speaker until the sensor is deactivated.
Make call to extension	Check this box to call a preset extension (once).
Play recorded audio	Check this box to play a pre-recorded audio file (once).
Dial Out Extension	Enter the desired dial-out extension number.
Extension ID	Type the desired Extension ID (64 character limit).
	Use this button to test the door sensor.
Intrusion Sensor Settings	
Flash Button LED*	Check this box to flash the LED until the sensor is deactivated (roughly 10 times/second).
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Play Audio Locally	Check this box to loop an audio file out of the Intercom speaker until the sensor is deactivated.
Make call to extension	Check this box to call a preset extension (once).
Play recorded audio	Check this box to play a pre-recorded audio file (once).
Dial Out Extension	Enter the desired dial-out extension number.
Extension ID	Type the desired Extension ID (64 character limit).
	Use this button to test the Intrusion sensor.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**.

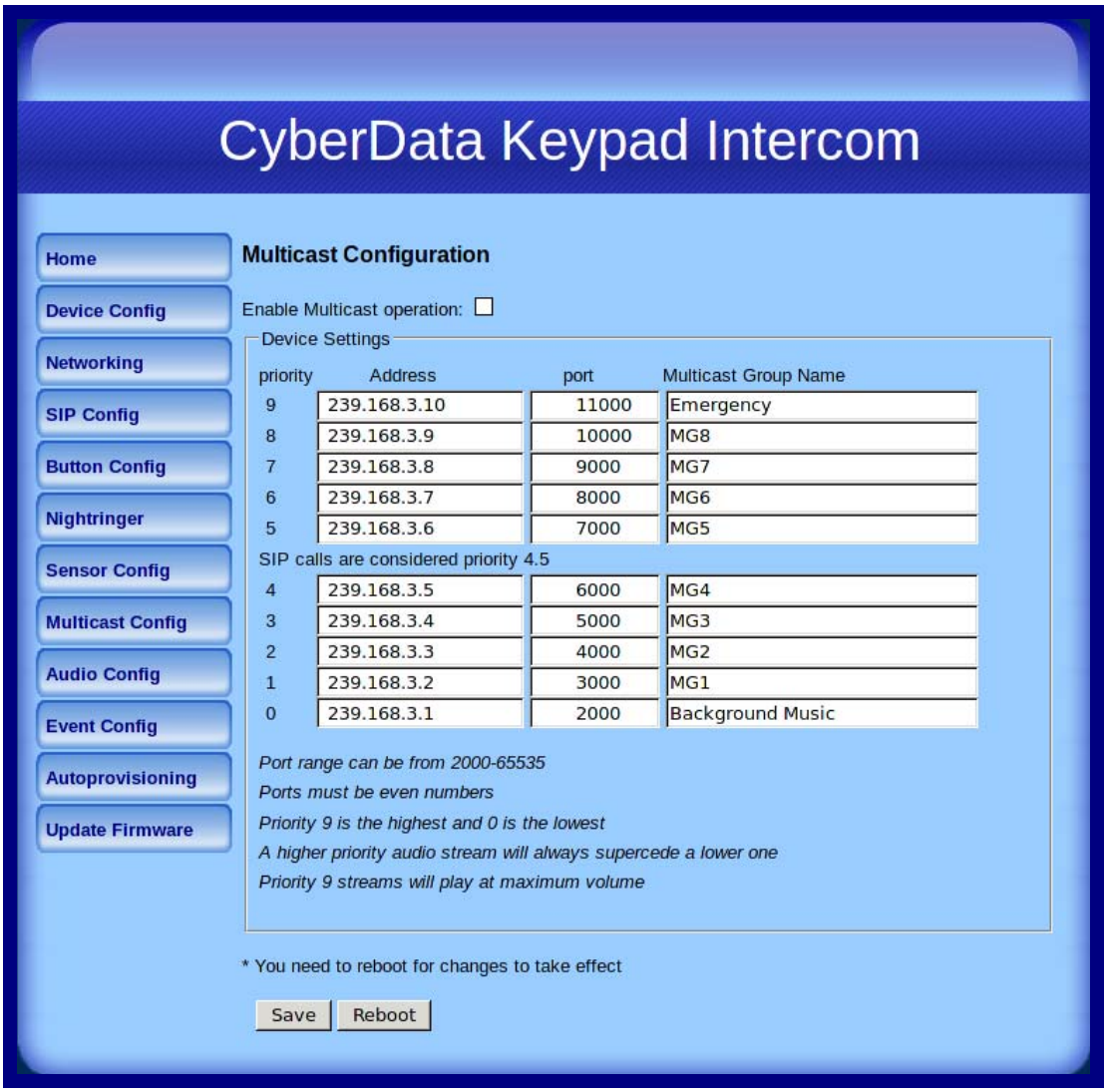
2.4.10 Configure the Multicast Parameters

Multicast groups use multicasting to create public address paging zones. Multicasting is based on the concept of a group. Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to the group. Group members send IGMP messages to their local multicast routers, allowing the group traffic traversal from the source.

Multicast configuration provides the ability to join up to 10 paging zones. A paging zone can consist of one, or many, CyberData multicast group-enabled devices. There is no limit to how many devices can be in a given paging zone. Each multicast group is defined by a multicast address and port number. Each multicast group is also assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The Intercom supports simultaneous SIP and Multicast.

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See Figure 2-20.

Figure 2-20. Multicast Configuration Setup



2. On the **Multicast Configuration** page, enter values for the parameters indicated in Table 2-16.

Table 2-16. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Device Settings	
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). See Section 2.4.10.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port (range can be from 2000 to 65535)	Enter the port number for this multicast group (5 character limit). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Multicast Group Name	Assign a descriptive name for this multicast group (25 character limit).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.4.10.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams the volume level is set to maximum.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

Ringtones and Nightringtones

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

2.4.11 Configure the Audio Parameters

The **Audio Configuration** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the Intercom.

1. Click **Audio Config** to open the **Audio Configuration** page (Figure 2-21).

Figure 2-21. Audio Configuration Page

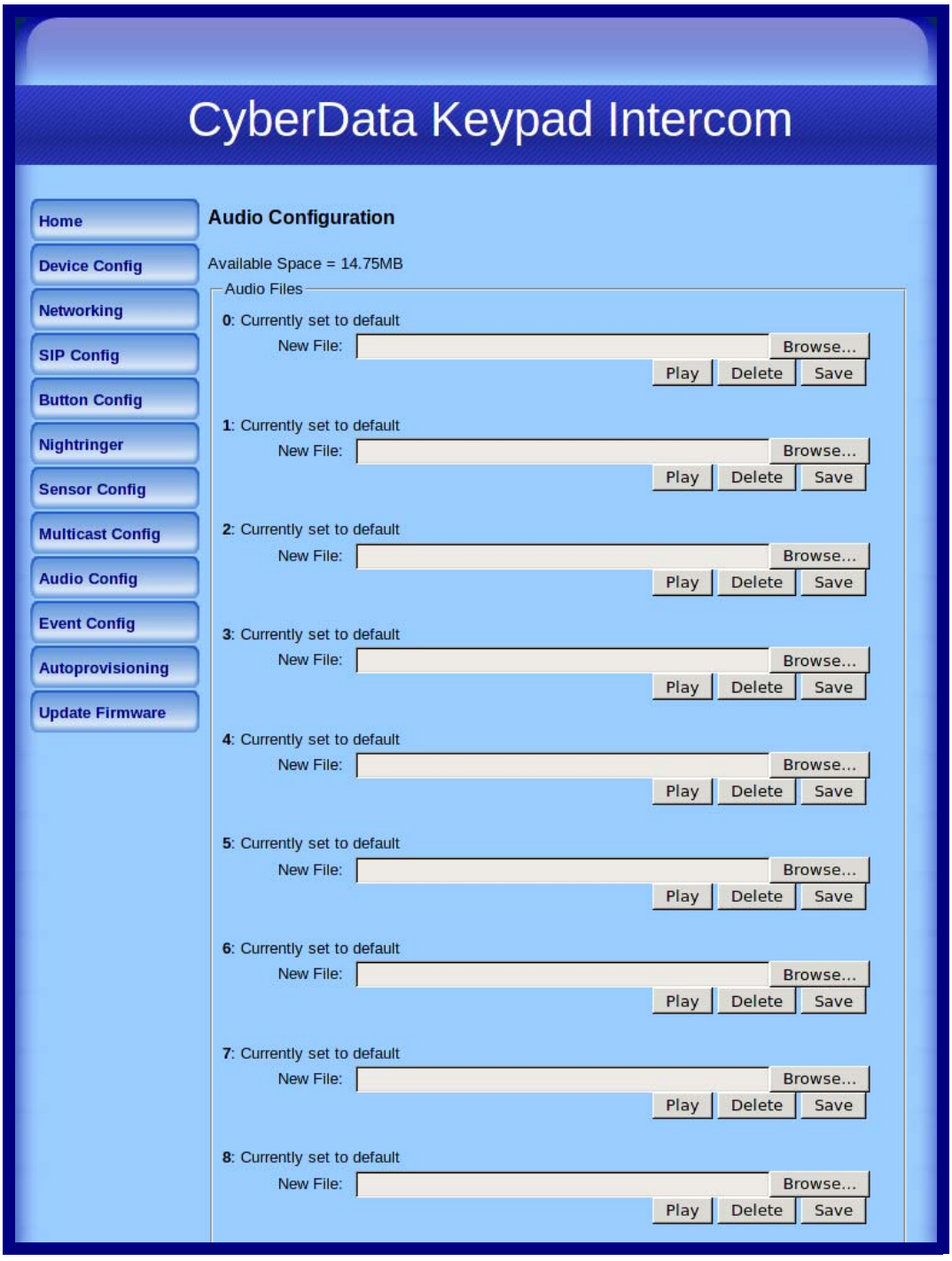
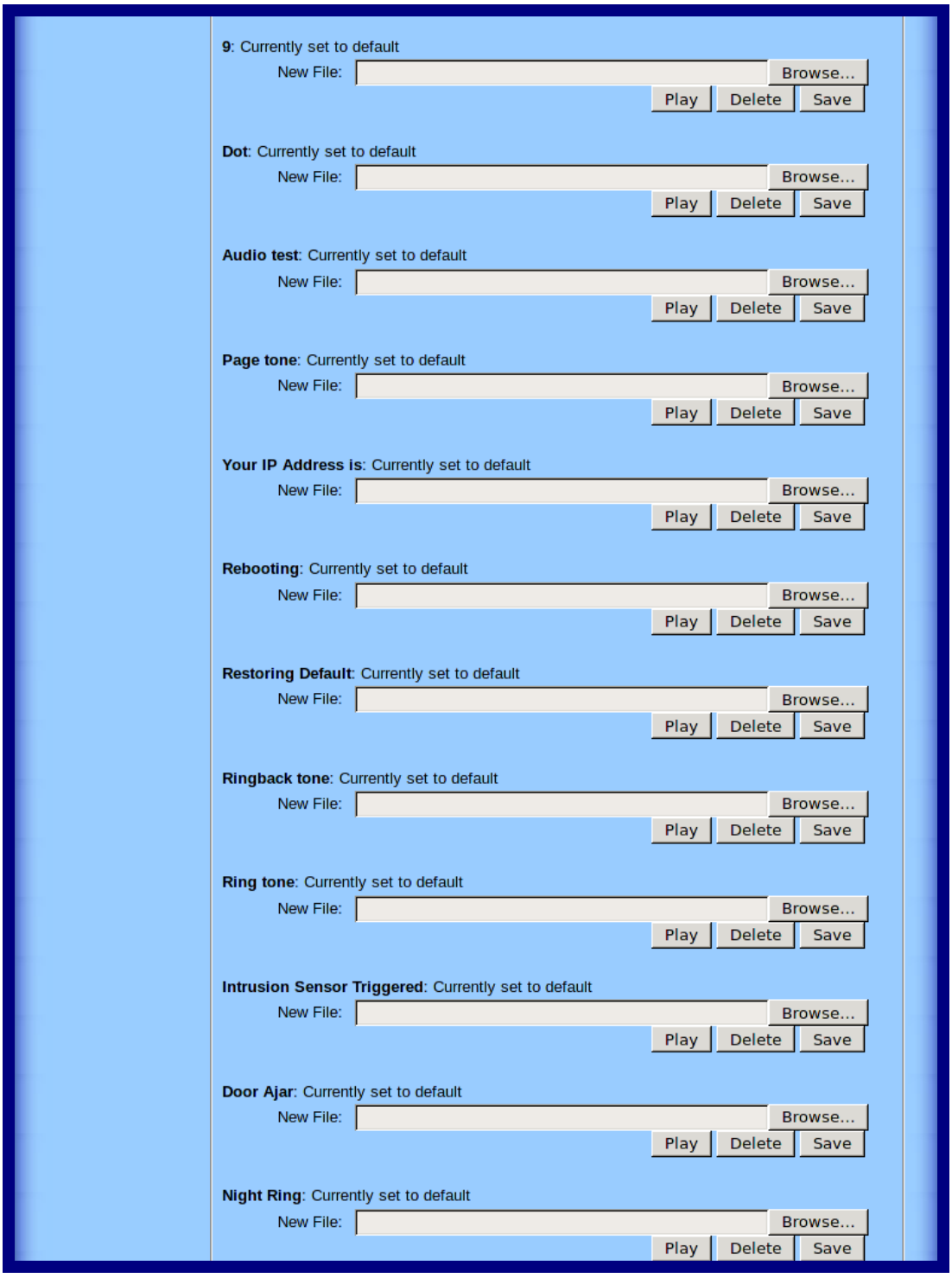


Figure 2-22. Audio Configuration Page (continued)



2. On the **Audio Configuration** page, enter values for the parameters indicated in Table 2-15.

Note Each entry on the **Audio Configuration** page replaces one of the stock audio files on the board. When the input box displays the word **default**, the Intercom is using the stock audio file. If that file is replaced with a user file, it will display the uploaded filename.

Table 2-17. Audio Configuration Parameters

Web Page Item	Description
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board. '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '5' corresponds to the spoken word “five.” '6' corresponds to the spoken word “six.” '7' corresponds to the spoken word “seven.” '8' corresponds to the spoken word “eight.” '9' corresponds to the spoken word “nine.”
Dot	Corresponds to the spoken word “dot.” (24 character limit)
Audiotest	Corresponds to the message “This is the CyberData IP speaker test message...” (24 character limit)
Pagetone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).
Restoring default	Corresponds to the message “Restoring default” (24 character limit).
Ringback Tone	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message “Intrusion sensor triggered.”
Door Ajar	Corresponds to the message “Door Ajar” (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
	The **Browse** button will allow you to navigate to and select an audio file.

Table 2-17. Audio Configuration Parameters (continued)

Web Page Item	Description
	The **Play** button will play that audio file.
	The **Delete** button will delete any user uploaded audio and restore the stock audio file.
	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

2.4.11.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-23 through Figure 2-25.

Figure 2-23. Audacity 1

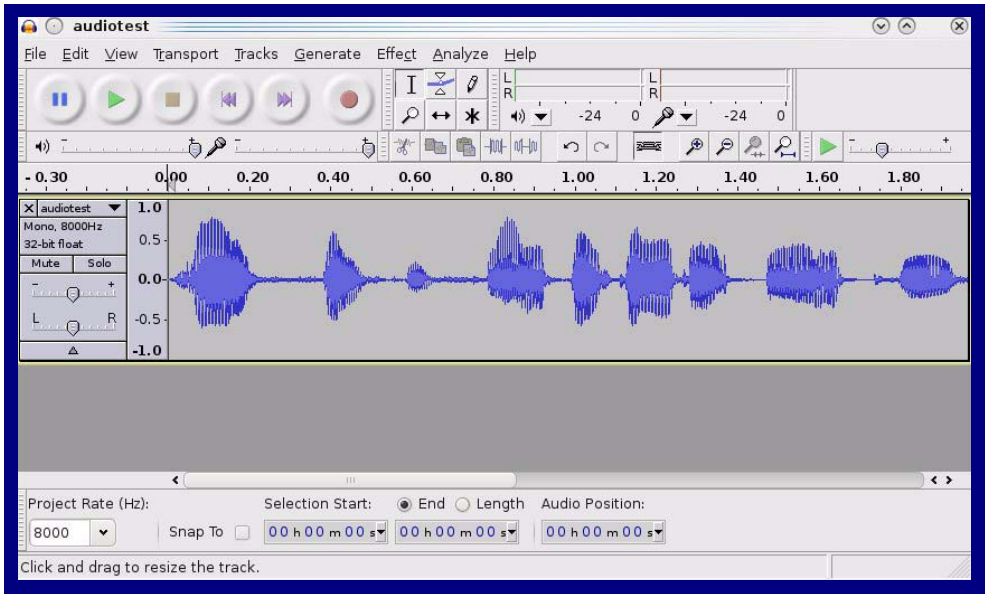
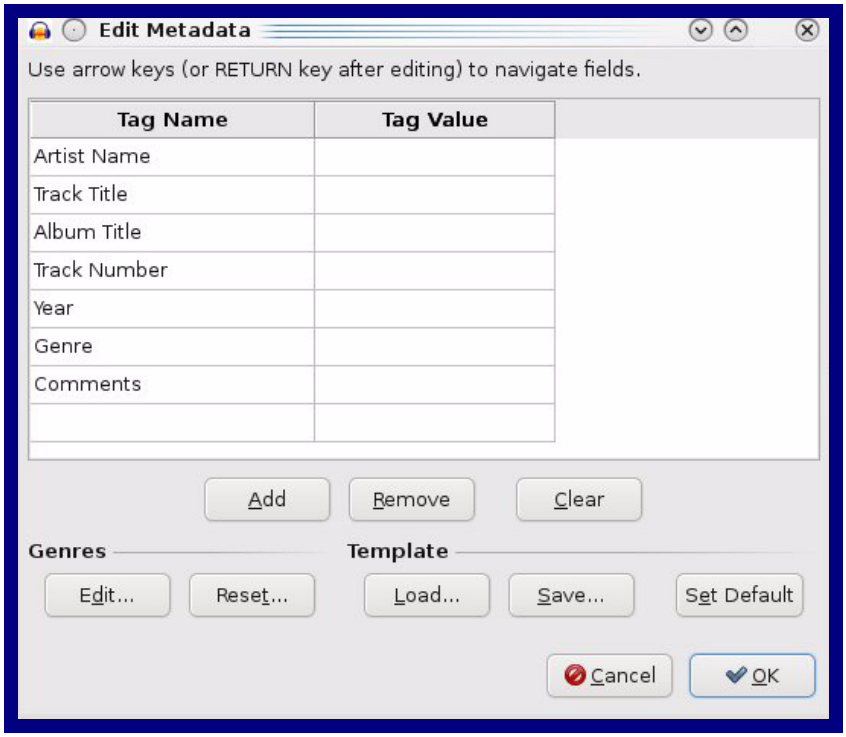


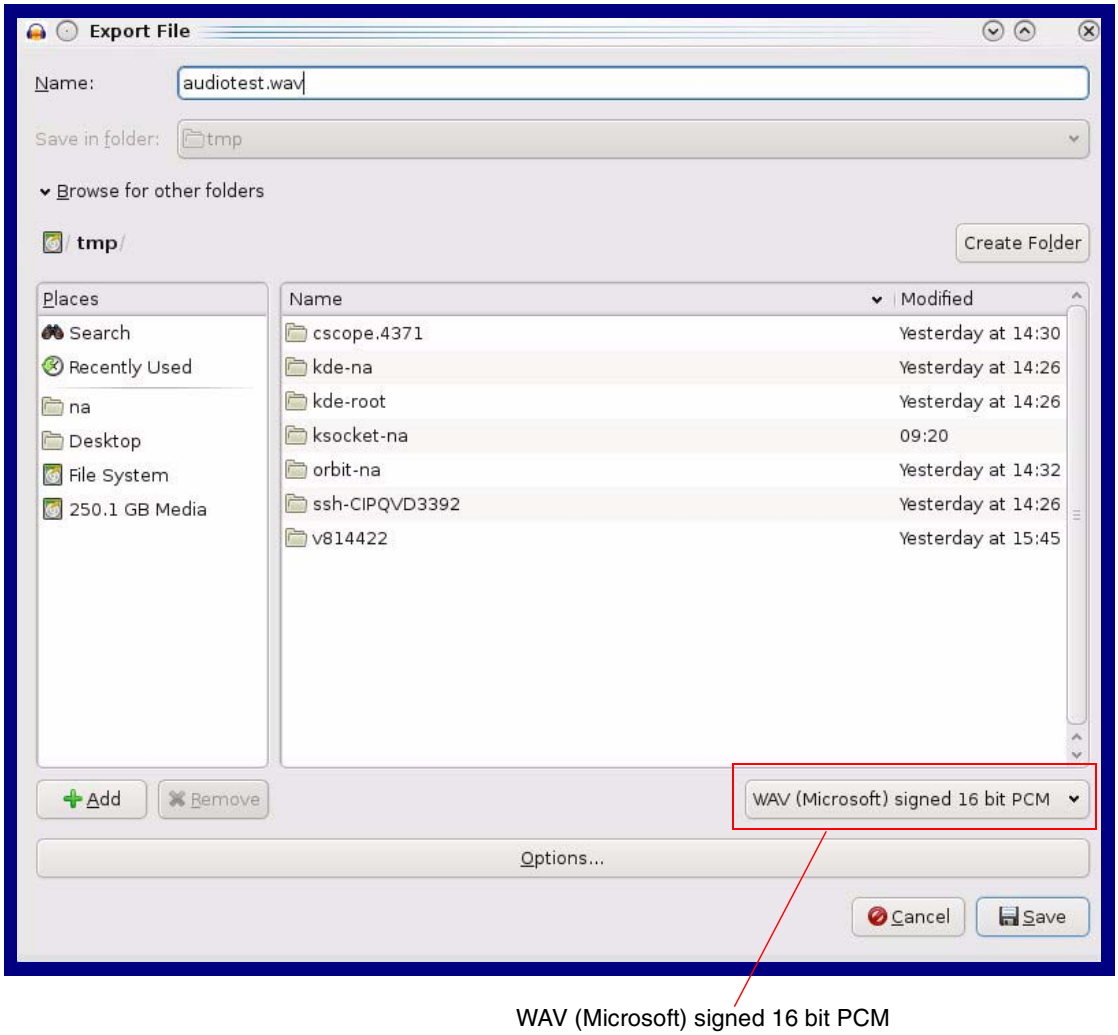
Figure 2-24. Audacity 2



When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM**.

Figure 2-25. WAV (Microsoft) signed 16 bit PCM



2.4.12 Configure the Event Parameters

Click the **Event Config** button to open the **Event Configuration** page. The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-26. Event Configuration Page

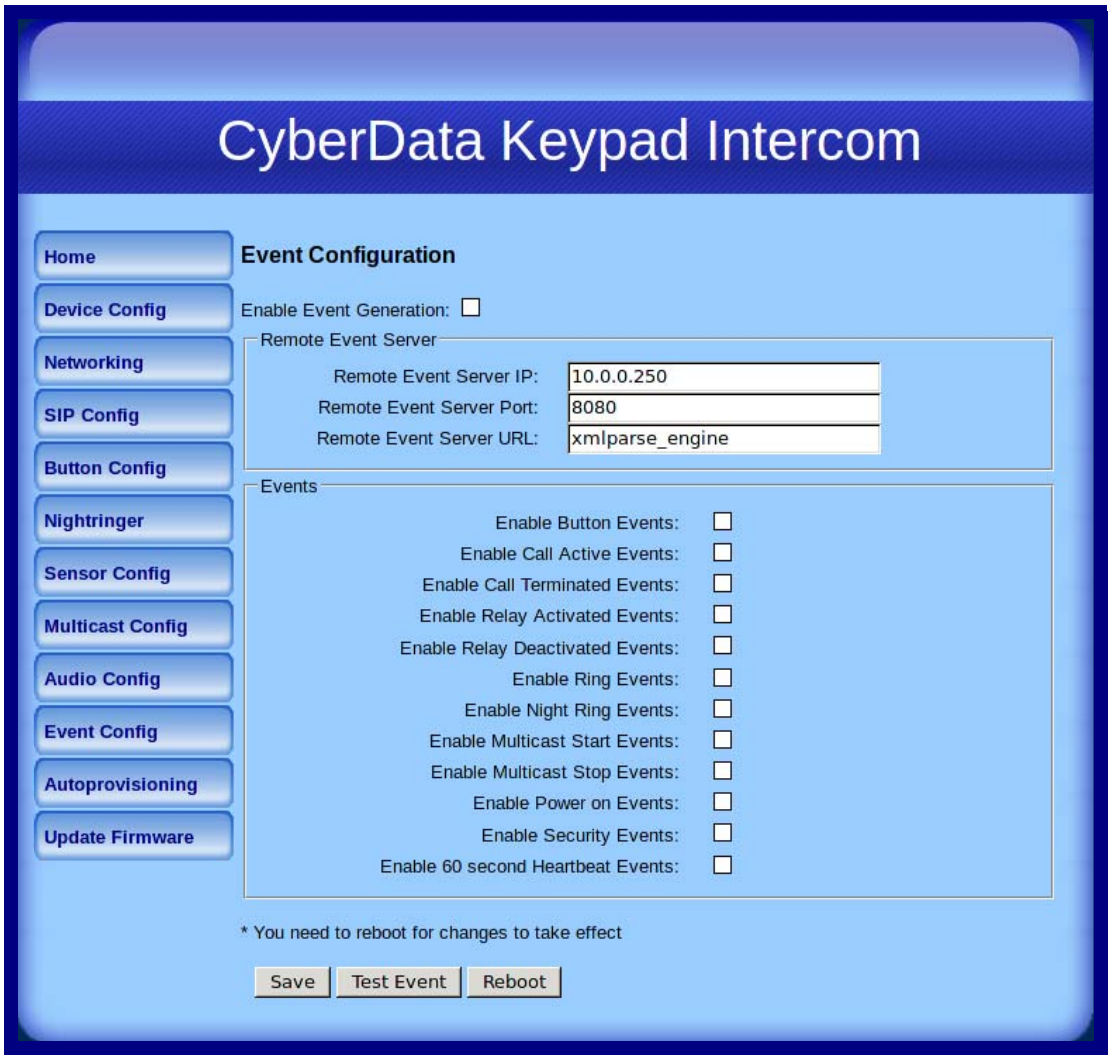


Table 2-18 shows the web page items on the **Event Configuration** page.

Table 2-18. Event Configuration

Web Page Item	Description
Enable Event Generation	When selected, Event Generation is enabled.
Remote Event Server	
Remote Event Server IP	Type the Remote Event Server IP address. (64 character limit)
Remote Event Server Port	Type the Remote Event Server port number. (8 character limit)
Remote Event Server URL	Type the Remote Event Server URL. (127 character limit)
Events	
Enable Button Events	When selected, Button Events are enabled.
Enable Call Active Events	When selected, Call Active Events are enabled.
Enable Call Terminated Events	When selected, Call Terminated Events are enabled.
Enable Relay Activated Events	When selected, Relay Activated Events are enabled.
Enable Relay Deactivated Events	When selected, Relay Deactivated Events are enabled.
Enable Ring Events	When selected, Ring Events are enabled.
Enable Night Ring Events	When selected, there is a notification when the device receives a night ring.
Enable Multicast Start Events	When selected, Multicast Start Events are enabled.
Enable Multicast Stop Events	When selected, Multicast Stop Events are enabled.
Enable Power On Events	When selected, Power On Events are enabled.
Enable Security Events	When selected, an event is sent every time a security code is entered on the keypad.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Test Event	Click on the **Test Event** button to test an event.
Reboot	Click on the **Reboot** button to reboot the system.

2.4.12.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
```

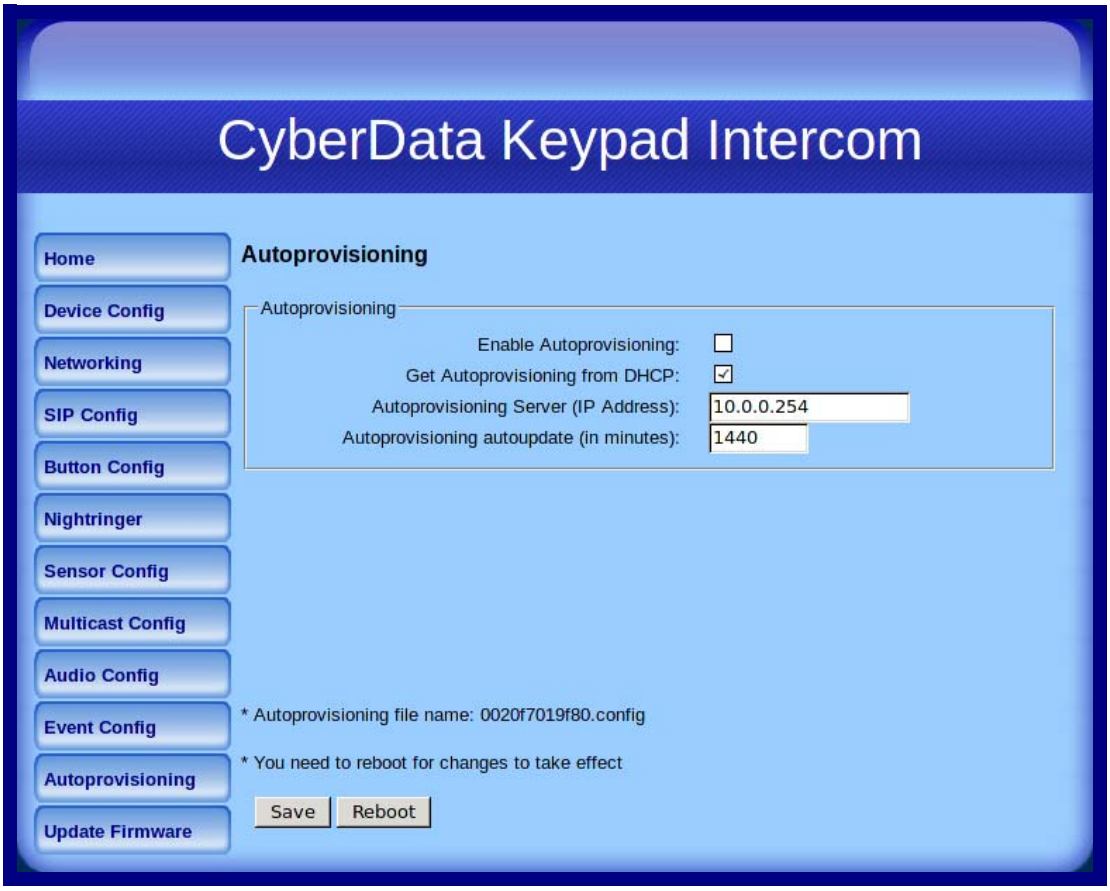
```
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>SECURITY</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWER ON</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>DOOR SENSOR</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>INTRUSION SENSOR</event>
<index>8</index>
</cyberdata>
```

2.4.13 Configure the Autoprovisioning Parameters

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page. See Figure 2-27.

Figure 2-27. Autoprovisioning Configuration Page



2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 2-19.

Table 2-19. Autoprovisioning Configuration Parameters

Web Page Item	Description
Autoprovisioning	
Enable Autoprovisioning	See Section 2.4.13.1, "Autoprovisioning".
Get Autoprovisioning from DHCP	See Section 2.4.13.1, "Autoprovisioning".
Autoprovisioning Server (IP Address)	See Section 2.4.13.1, "Autoprovisioning" (15 character limit).
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.4.13.1 Autoprovisioning

Enable Autoprovisioning Option

With autoprovisioning enabled, the board will get its configuration from a remote TFTP server on startup or periodically on a scheduled delay. Autoprovisioned values will override values stored in on-board memory and will be visible on the web page. The board gets its autoprovisioning information from an XML-formatted file hosted from a TFTP server. CyberData will provide a template for this XML file and the user can modify it for their own use.

To use autoprovisioning, create a copy of the autoprovisioning template with the desired settings and name this file with the mac address of the device to configure (for example: **0020f7350058.config**). Put this file into your TFTP server directory and manually set the TFTP server address on the board.

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <MiscSettings>
        <DeviceName>auto Intercom</DeviceName>
    </MiscSettings>

</specific>
```

Networking

The board will only apply networking settings or firmware upgrades after a reboot.

Get Autoprovisioning from DHCP

When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.

To set up a Linux DHCPD server to serve autoprovisioning information (in this case using option 150), here's an example:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
        max-lease-time 120;
        default-lease-time 120;

        option routers                  10.0.0.1;
        option subnet-mask              255.0.0.0;

        option domain-name              "voiplab";
        option domain-name-servers       10.0.0.1;

        option time-offset              -8;     # Pacific Standard Time

        option tftp-server-name         "10.0.0.254";

        option option-150               10.0.0.254;

        range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address)

Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate

If **Autoprovisioning** is enabled and the **Autoprovisioning Autoupdate** value is something other than **0** minutes, a service is started on startup that will wait the configured number of minutes and then try to re-download its autoprovisioning file. It will compare its previously autoprovisioned file with this new file and if there are differences, it will reboot the board.

Autoprovisioned Firmware Upgrades

An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion**' value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v6.3.0</FirmwareVersion>
<FirmwareFile>630-keypadintercom-uImage</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio Configuration** page or by changing the autoprovisioning file with "**default**" set as the file name.

2.5 Upgrade the Firmware and Reboot the Intercom

Caution

Equipment Hazard: V3 devices like the VoIP V3 Outdoor Intercom with Keypad cannot use firmware 6.x.x or earlier, and older V1 and V2 devices cannot use firmware 7.x.x or later.

To upload the firmware from your computer:

1. Retrieve the latest Intercom firmware file from the VoIP V3 Outdoor Intercom with Keypad **Downloads** page at:

   http://www.cyberdata.net/products/voip/digitalanalog/intercomkeypadv3/downloads.html

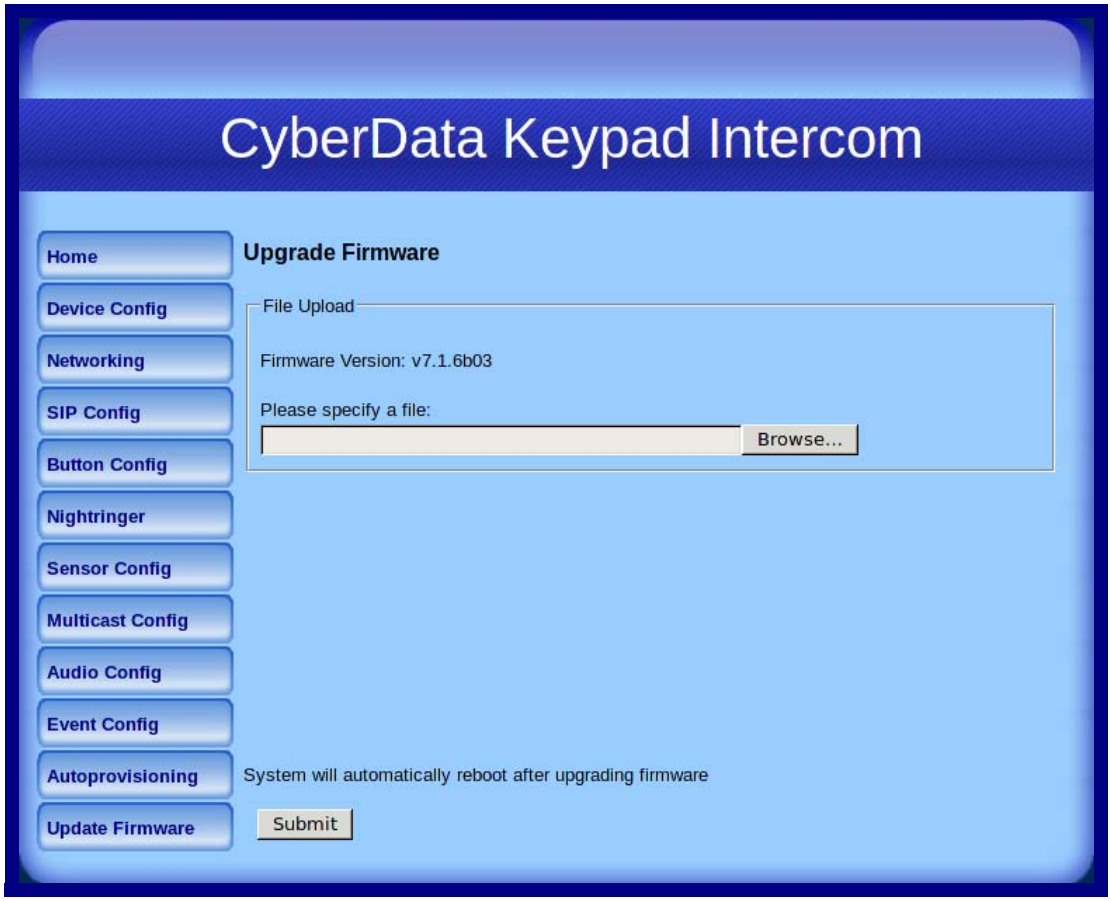
2. Unzip the firmware version file. This file may contain the following:

- Firmware file
- Release notes

3. Log in to the Intercom home page as instructed in Section 2.4.3, "Log in to the Configuration Home Page".

4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See Figure 2-28.

Figure 2-28. Upgrade Firmware Page



5. Select **Browse**, and then navigate to the location of the Intercom firmware file.
6. Click **Submit**.

Note This starts the upgrade process. Once the Intercom has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Intercom will automatically reboot when the upload is complete. When the countdown finishes, the **Upgrade Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

Table 2-20 shows the web page items on the **Upgrade Firmware** page.

Table 2-20. Firmware Upgrade Parameters

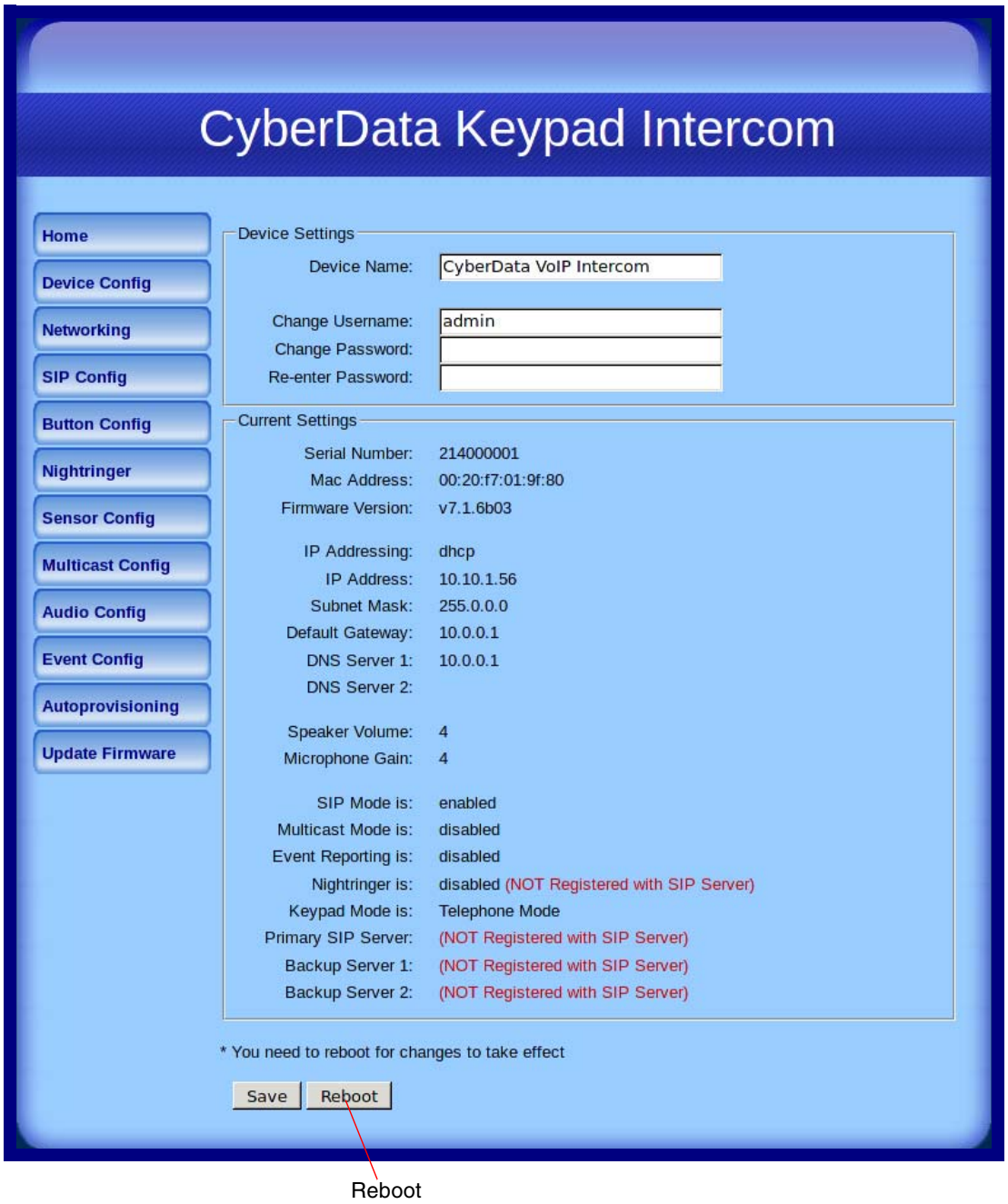
Web Page Item	Description
File Upload	
Firmware Version	Shows the current firmware version.
Browse...	Use the **Browse** button to navigate to the location of the Intercom firmware file that you want to upload.
Submit	Click on the **Submit** button to automatically upload the selected firmware and reboot the system.

2.5.1 Reboot the Intercom

To reboot a Intercom, log in to the web page as instructed in Section 2.4.3, "Log in to the Configuration Home Page".

1. Click **Reboot** (Figure 2-29). A normal restart will occur.

Figure 2-29. Reboot System Section



2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-21 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.6.1 Command Interface Post Commands

Note These commands require an authenticated session (a valid username and password to work).

Table 2-21. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Place point-to-point call[b] (example: IP phone address = 10.0.3.72)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=10.0.3.72"
Terminate active call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_3=yes"

Table 2-21. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_6=yes"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_d=yes"
Play the "Audio Test" audio file (from Audio Config)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_audiotest=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_restoringdefault=yes"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringback=yes"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringtone=yes"
Play the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_intrusionsensortriggered=yes"
Play the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_doorajar=yes"

Table 2-21. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_nightring=yes"
Delete the "0" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_0=yes"
Delete the "1" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_1=yes"
Delete the "2" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_2=yes"
Delete the "3" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_3=yes"
Delete the "4" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_4=yes"
Delete the "5" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_5=yes"
Delete the "6" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_6=yes"
Delete the "7" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_7=yes"
Delete the "8" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_8=yes"
Delete the "9" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_9=yes"
Delete the "Audio Test" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_audiotest=yes"
Delete the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_pagetone=yes"
Delete the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_youripaddressis=yes"
Delete the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_rebooting=yes"
Delete the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_restoringdefault=yes"

Table 2-21. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Delete the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringback=yes"
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringtone=yes"
Delete the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_intrusionsensortriggered=yes"
Delete the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_doorajar=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_nightring=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "intrusiontest=yes"

a.Type and enter all of each http POST command on one line.
b. Must be in point-to-point mode see Section 2.4.6.1, "Point-to-Point Configuration"

Appendix A: Mounting the VoIP V3 Outdoor Intercom with Keypad

A.1 Mount the Intercom

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to Table A-1. See Table A-2 and Table A-3 for optional accessories.

Table A-1. Mounting Components (Part of the Accessory Kit)

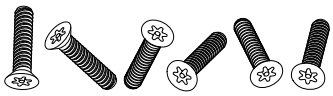
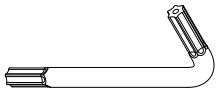
Quantity	Part Name	Illustration
6	Accessory Kit Security Torx MS	
1	Mounting Component Security Torx Key	

Table A-2. Optional Accessories (for gooseneck mounting)

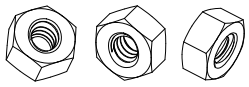
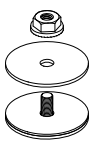
Quantity	Part Name	Illustration
3	Carriage bolt nuts	
3	Carriage bolts	
3	Carriage bolt washers	

Table A-3. Optional Accessories

Quantity	Part Name	Illustration
1	Spacer for Half-inch Set Screw Connector	
1	531085B Hole Plug Assembly	

A.2 Dimensions

Figure A-1. Unit Dimensions—Front and Side View

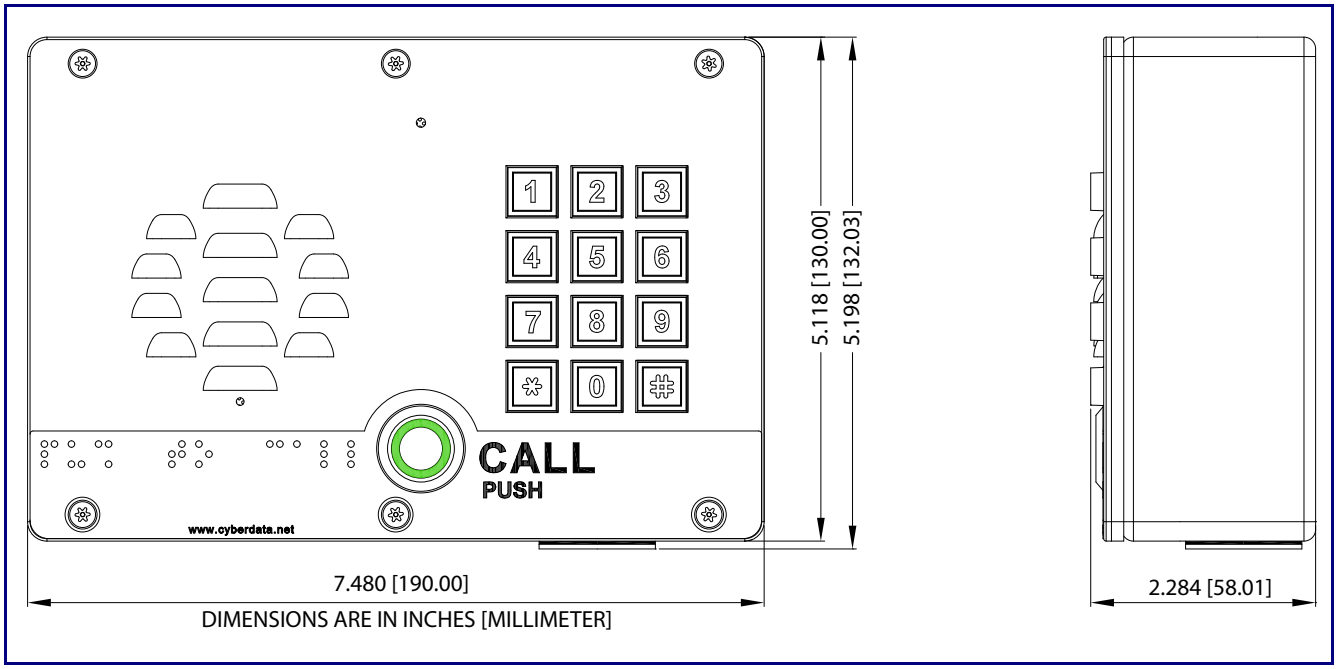


Figure A-1. Unit Dimensions—Rear View with Mounting Hole Locations

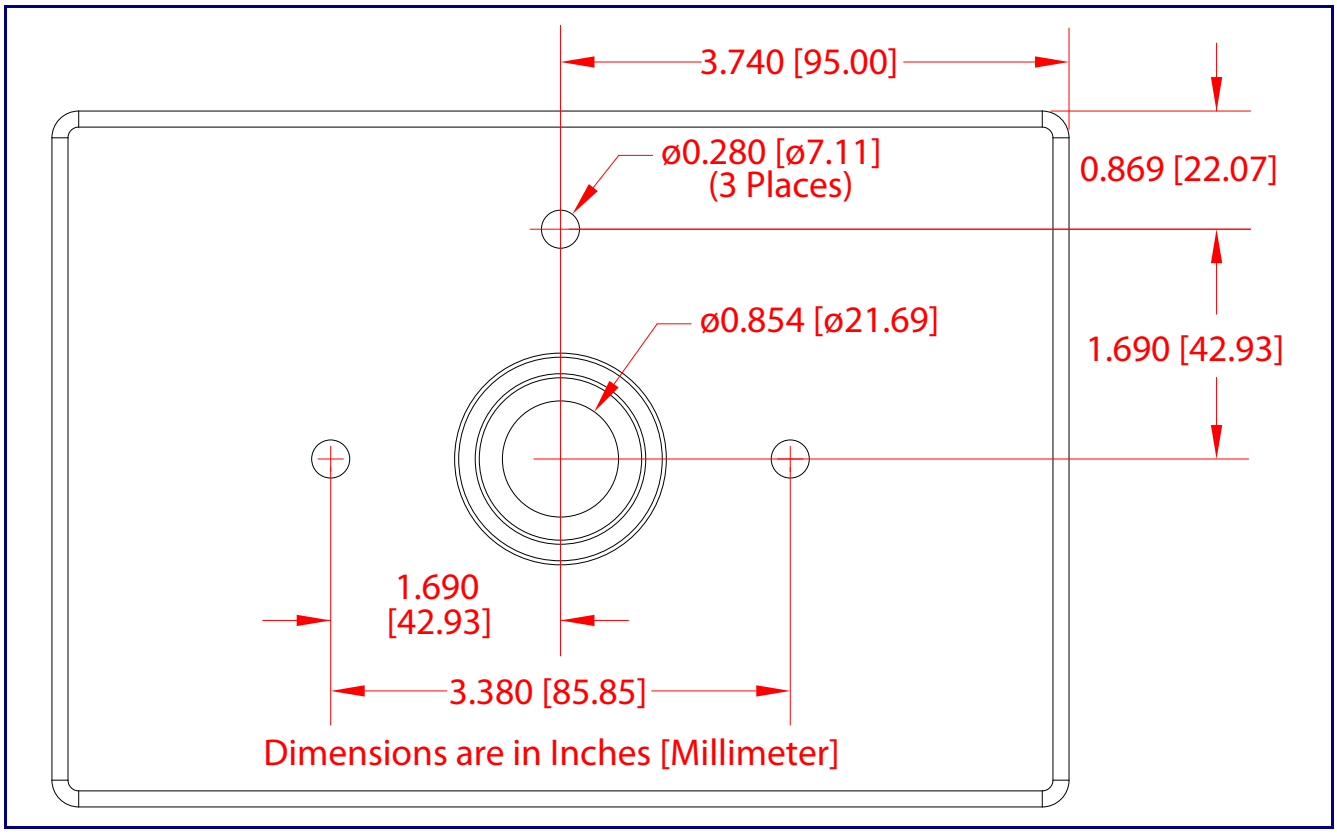


Figure A-2. Shroud Dimensions and Mounting Hole Locations

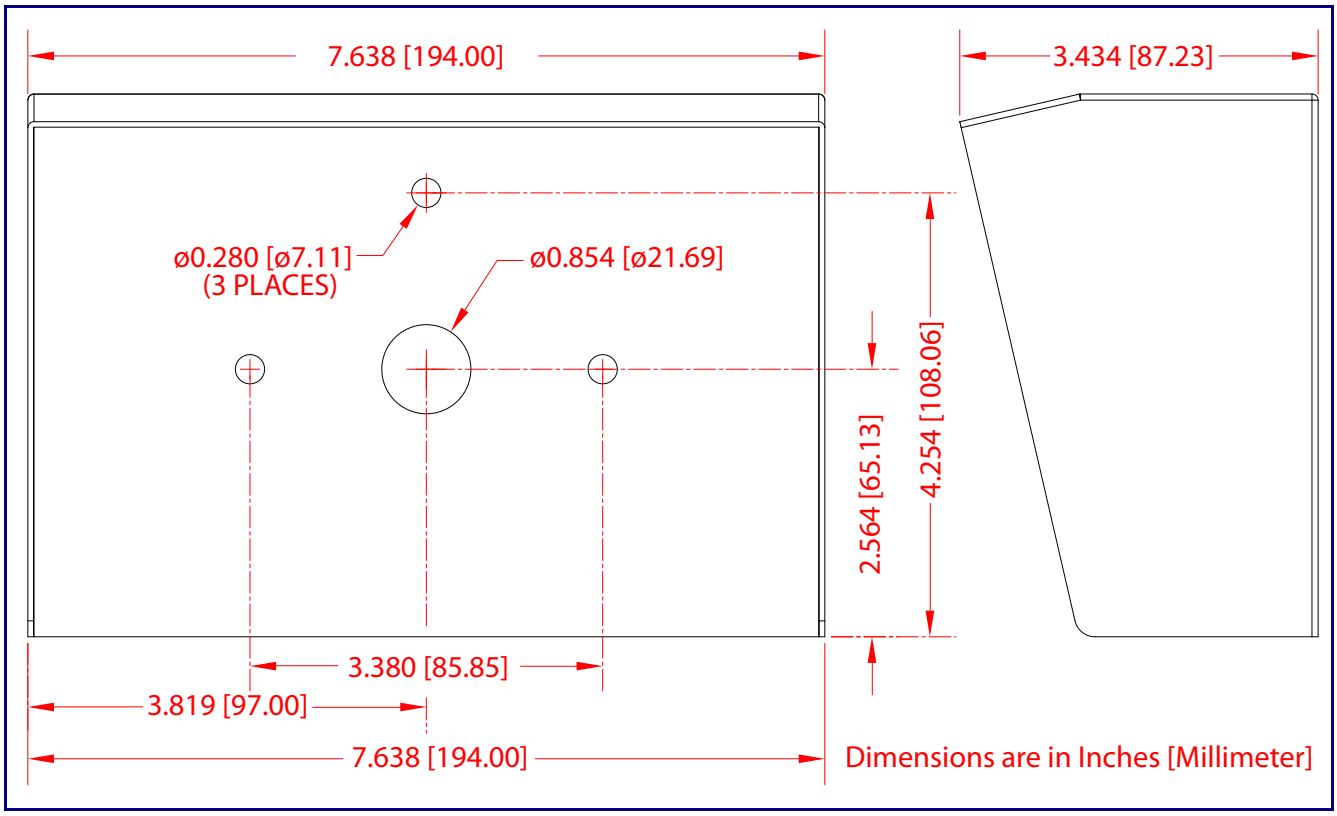


Figure A-3. Unit Dimensions—Intrusion Sensor Range and Unit without the Gang Box

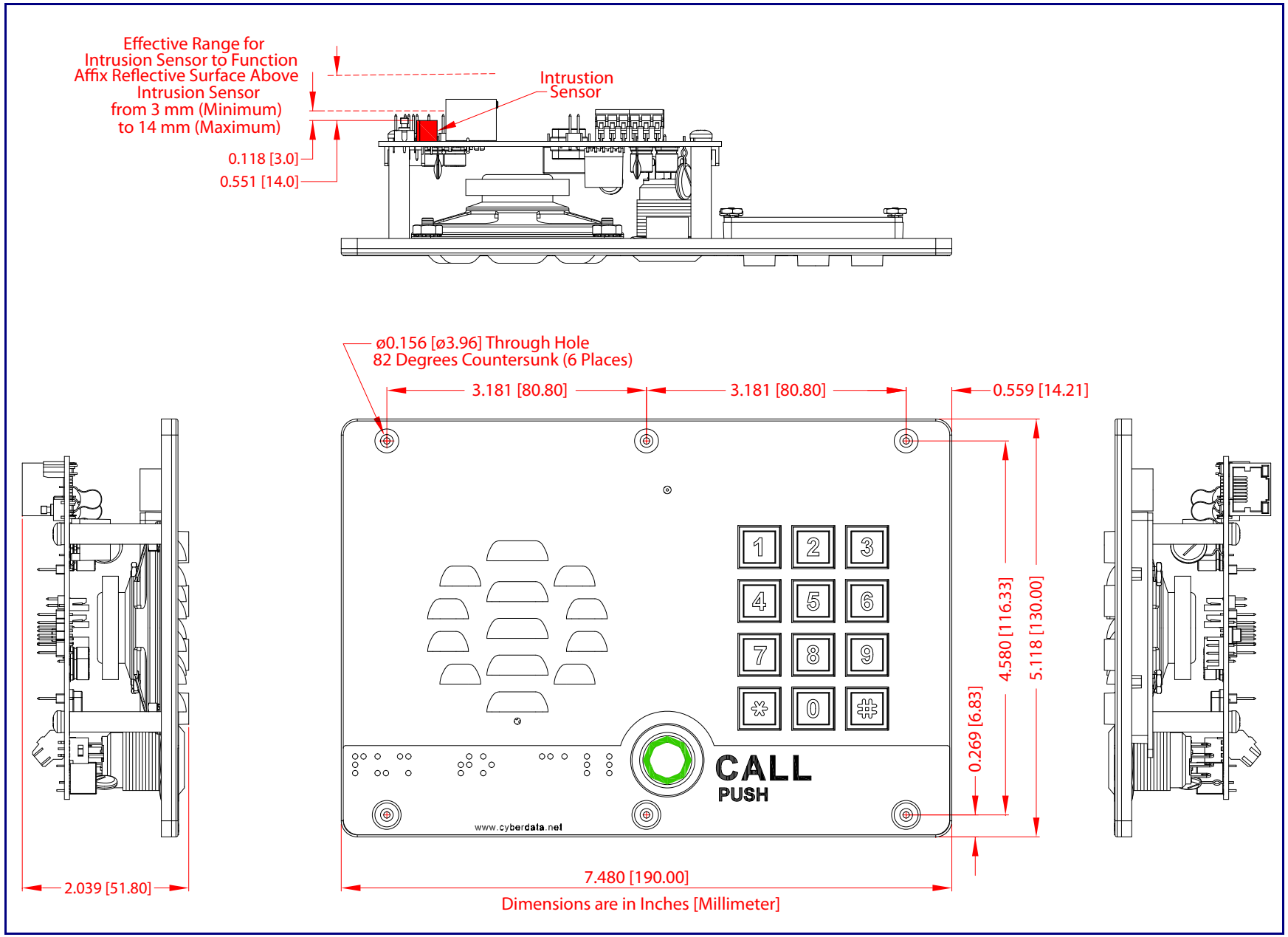
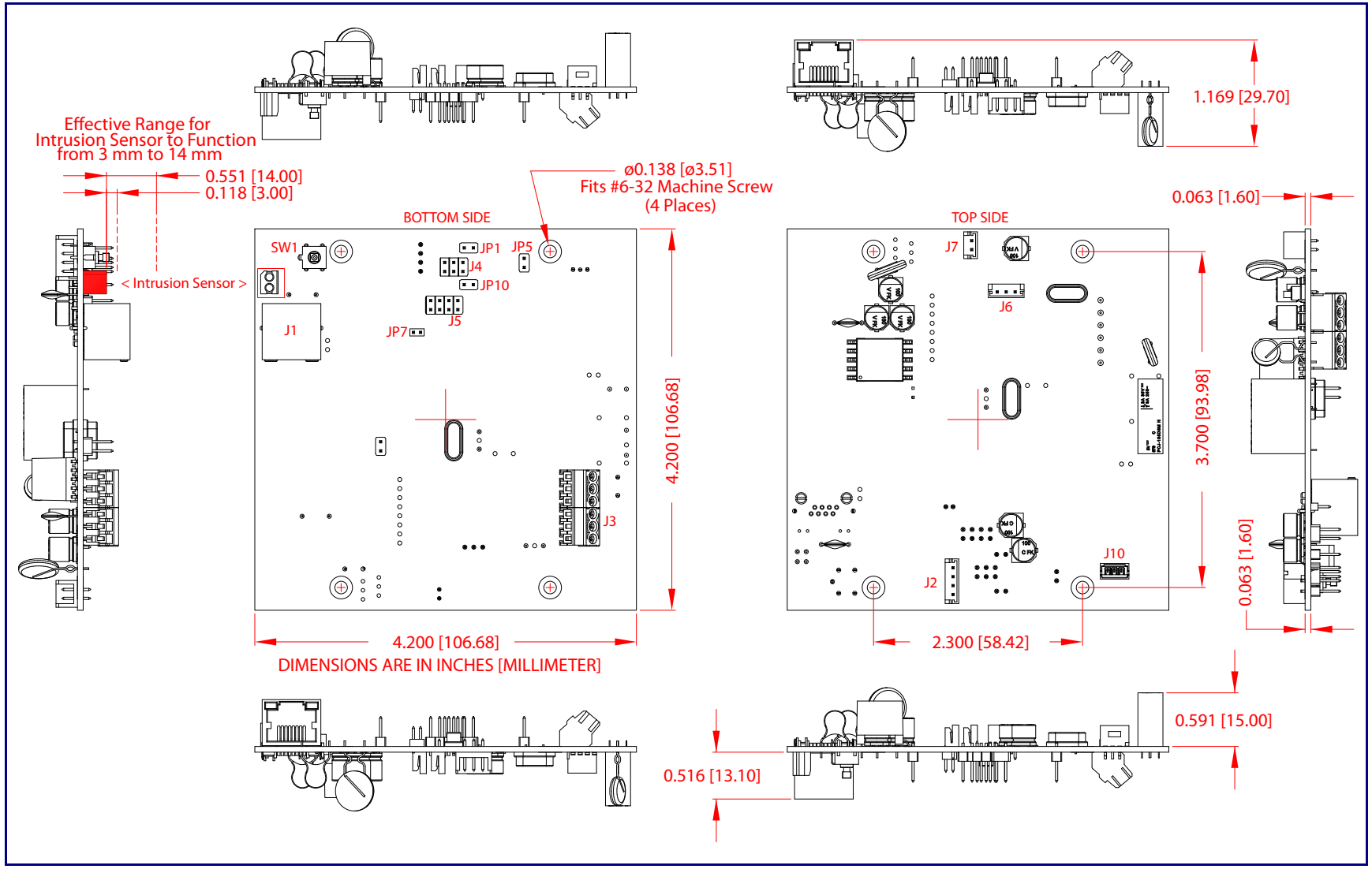


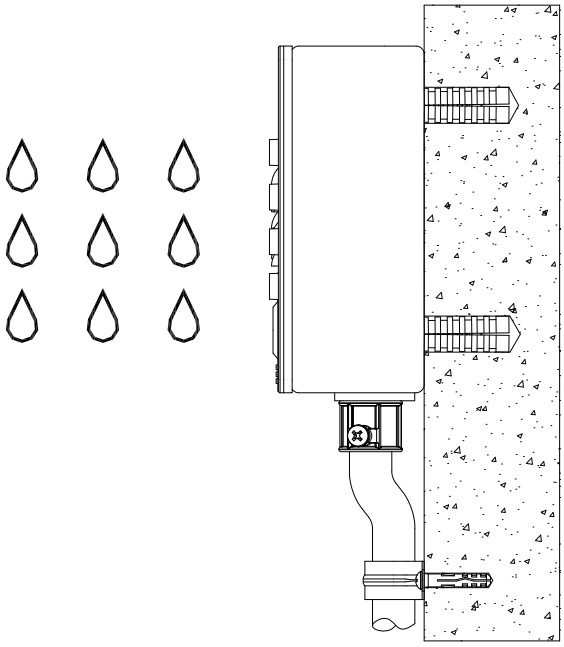
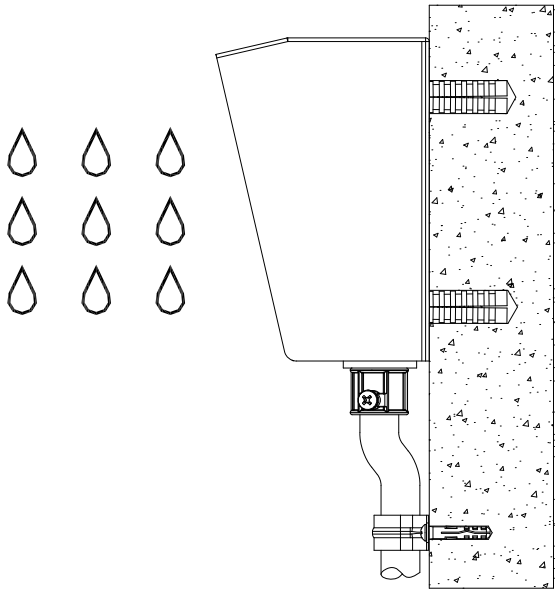
Figure A-4. PCB Dimensions and Intrusion Sensor Range



A.3 Overview of Installation Types

An overview of the installation types and the required components are provided in Table A-4.

Table A-4. Overview of Installation Types

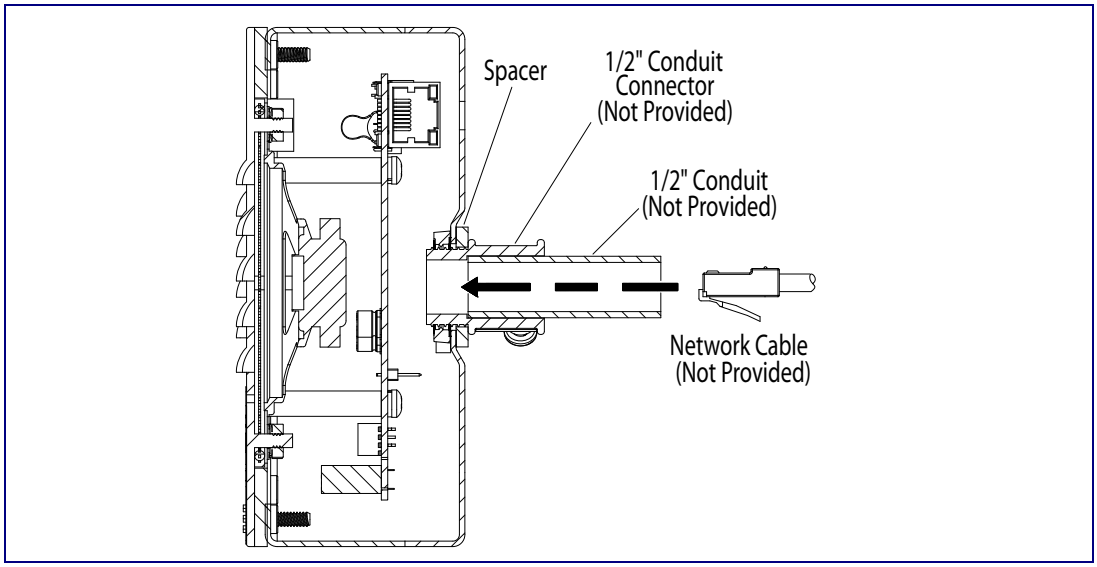
Installation Type	What You Need
Outdoor, on surface	
	011214 Intercom only
Outdoor, on surface with shroud (increased resistance)	
	011214 Intercom 011215 Weather Shroud (sold separately)

A.4 Network Cable Entry Restrictions

A.4.1 Rear Conduit Network Cable Entry Restrictions (without Shroud)

See Figure A-5 for the rear conduit cable entry restrictions (without Shroud).

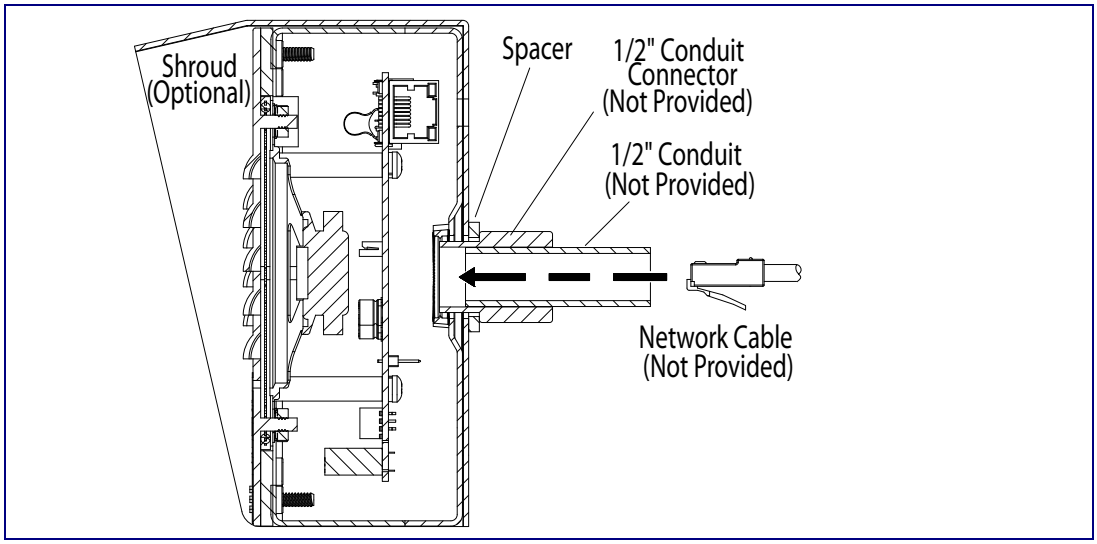
Figure A-5. Rear Conduit Network Cable Entry Restrictions—Without Shroud



A.4.2 Rear Conduit Network Cable Entry Restrictions (with Shroud)

See Figure A-6 for the rear conduit cable entry restrictions (with shroud).

Figure A-6. Rear Conduit Network Cable Entry Restrictions—With Shroud



A.5 Service Loop Cable Routing

Figure A-7 and Figure A-8 illustrate how to route the cables to the Intercom to create a service loop.

Figure A-7. Ground Cable Service Loop Routing

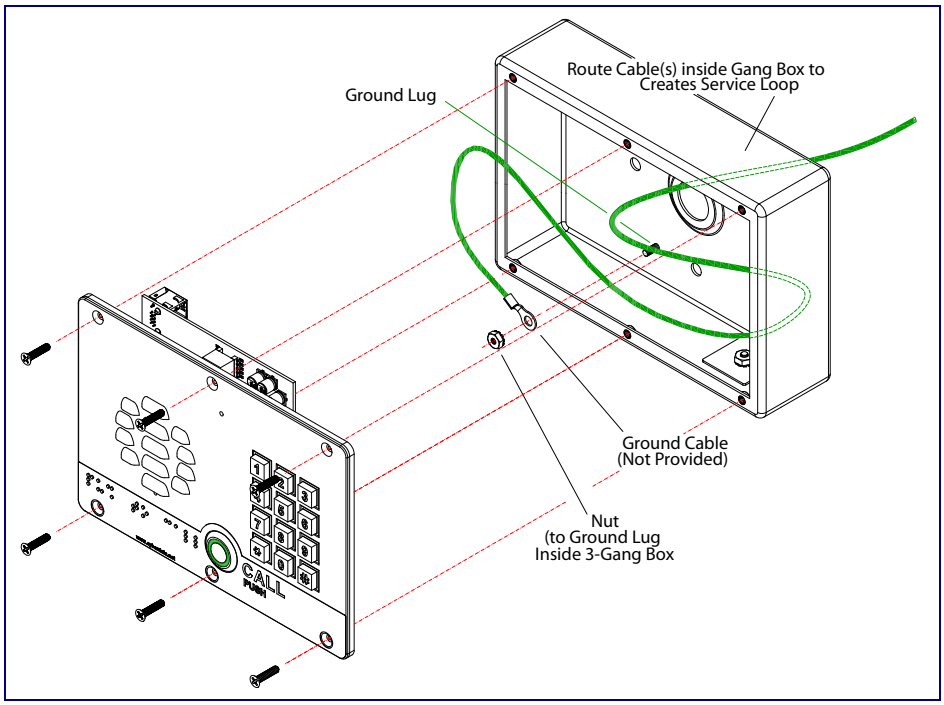
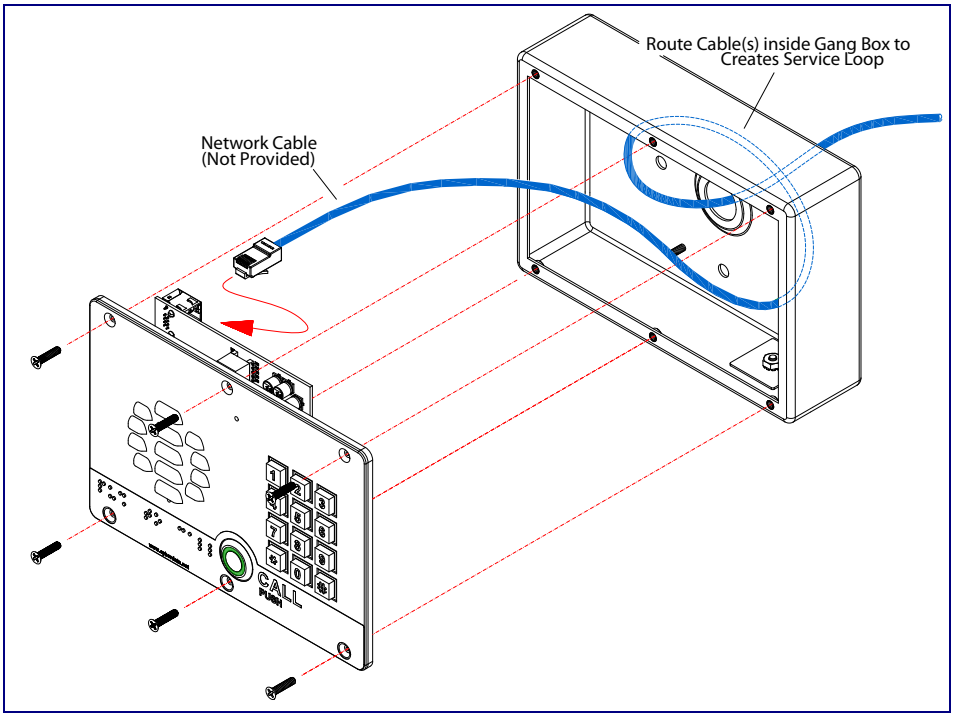


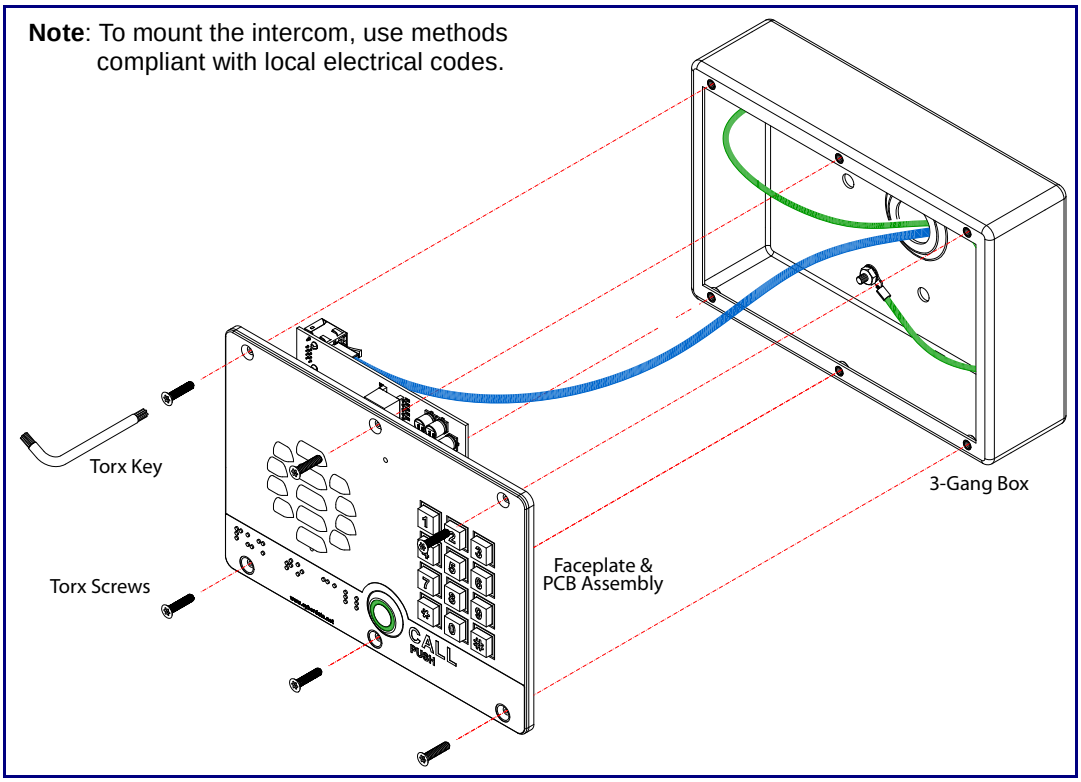
Figure A-8. Network Cable Service Loop Routing



A.6 Securing the Intercom

Use the four Security Torx screws to secure the Intercom. See Figure A-9.

Figure A-9. Securing the Intercom



GENERAL ALERT

Caution

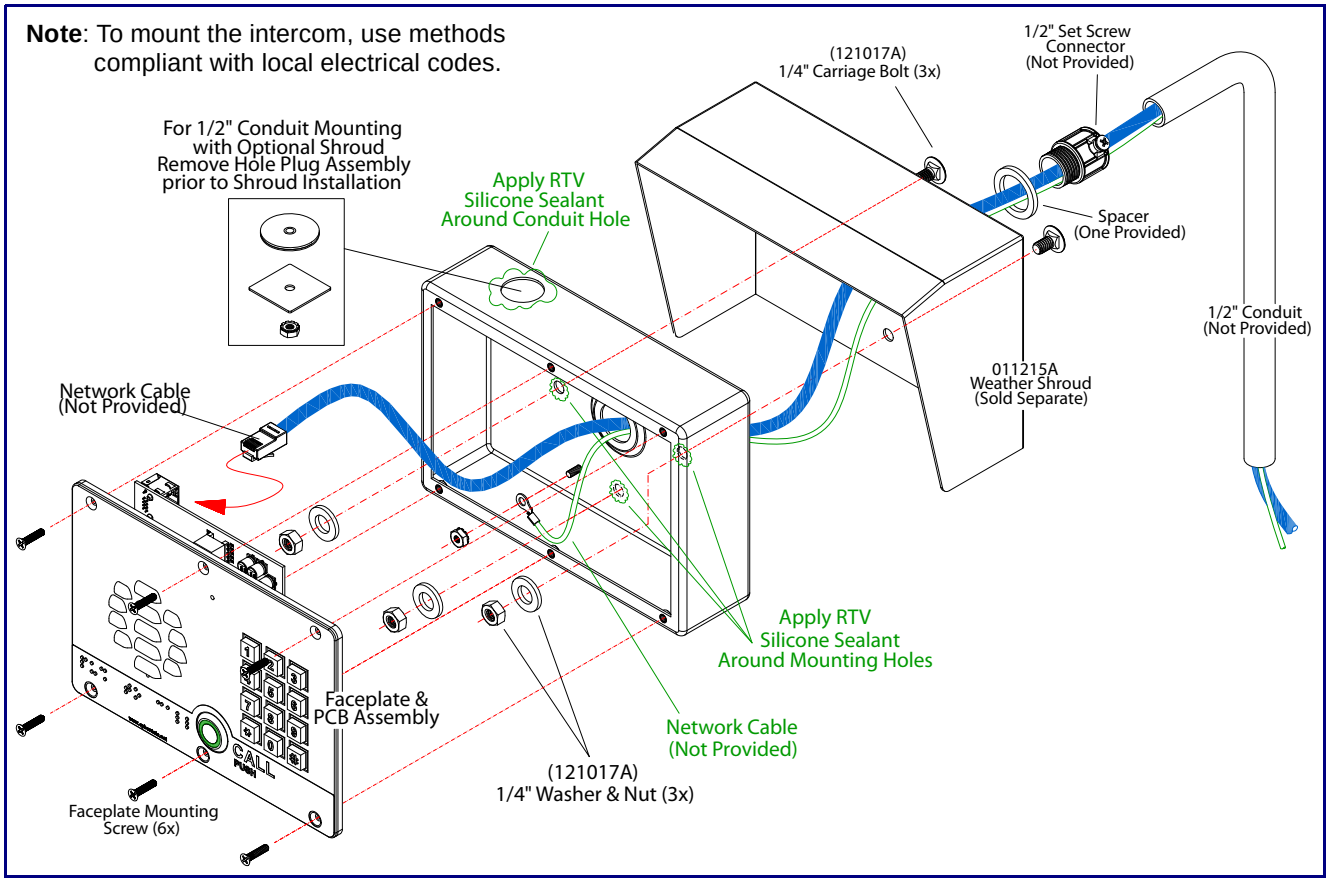
Equipment Hazard: Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void the manufacturer's warranty.

A.7 Additional Mounting Options

A.7.1 Rear Conduit Mounting Option (Not Provided)

Figure A-10 illustrates a rear conduit mounting option for the VoIP V3 Outdoor Intercom with Keypad.

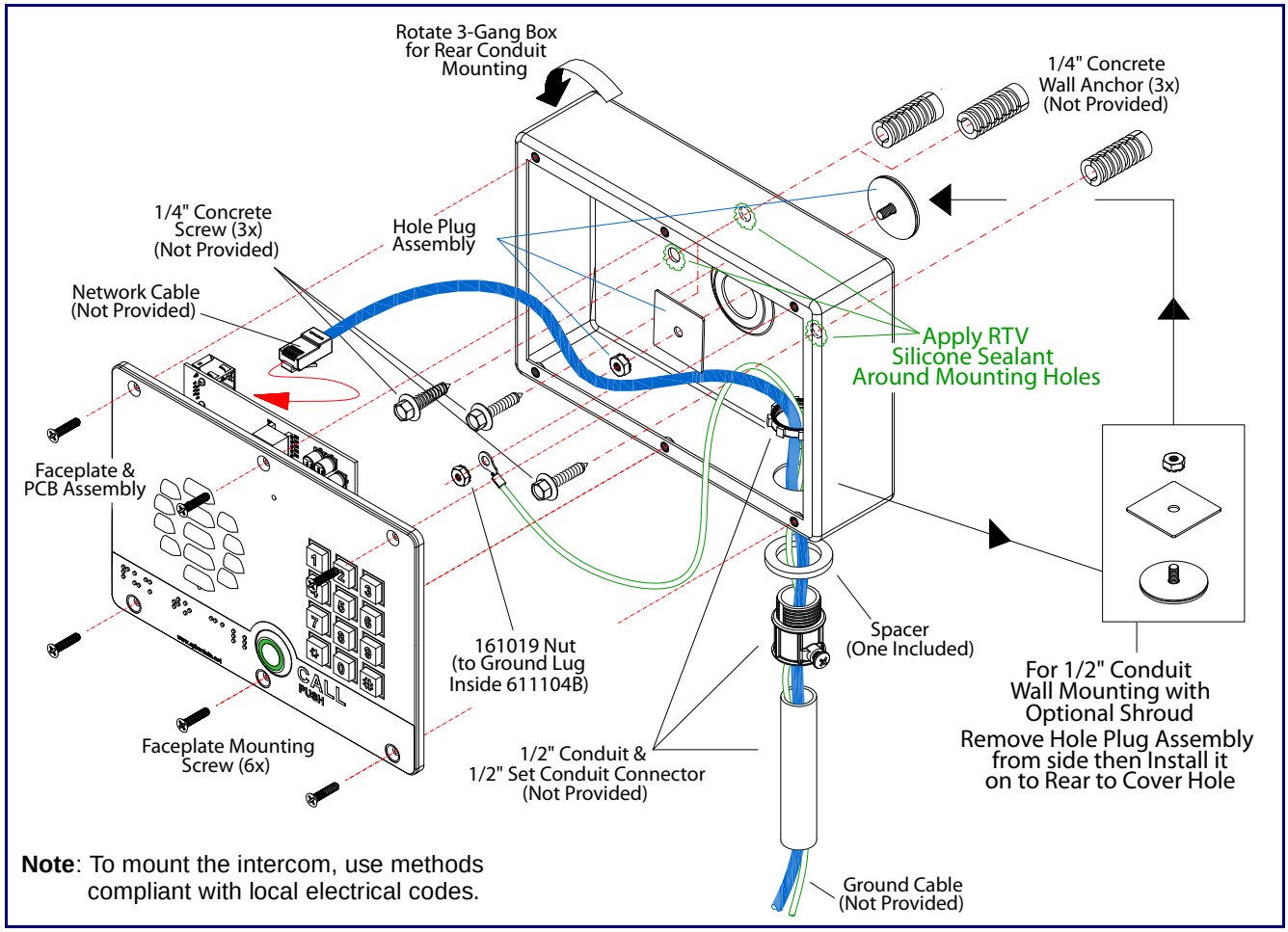
Figure A-10. Optional Rear Conduit Mounting



A.7.2 Concrete Wall Mounting Option (Not Provided)

Figure A-11 illustrates a concrete wall mounting option for the VoIP V3 Outdoor Intercom with Keypad.

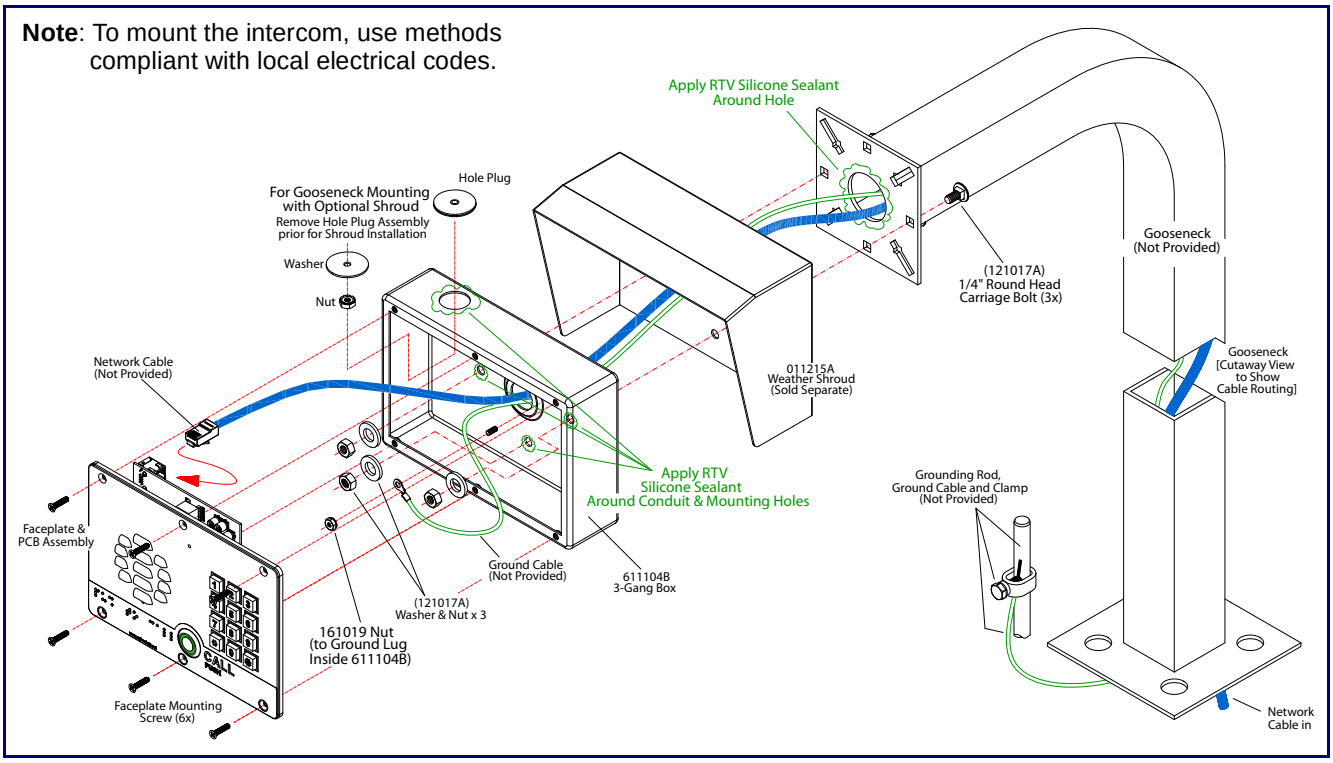
Figure A-11. Optional Concrete Wall Mounting


Rotate 3-Gang Box for Rear Conduit Mounting
1/4" Concrete Wall Anchor (3x) (Not Provided)
1/4" Concrete Screw (3x) (Not Provided)
Hole Plug Assembly
Network Cable (Not Provided)
Apply RTV Silicone Sealant Around Mounting Holes
Faceplate & PCB Assembly
161019 Nut (to Ground Lug Inside 611104B)
Spacer (One Included)
For 1/2" Conduit Wall Mounting with Optional Shroud
Remove Hole Plug Assembly from side then Install it on to Rear to Cover Hole
Faceplate Mounting Screw (6x)
1/2" Conduit & 1/2" Set Conduit Connector (Not Provided)
Ground Cable (Not Provided)
Note: To mount the intercom, use methods compliant with local electrical codes.

A.7.3 Goose Neck Mounting Option (Not Provided)

Figure A-12 illustrates a gooseneck mounting option for the VoIP V3 Outdoor Intercom with Keypad.

Figure A-12. Optional Goose Neck Mounting


Note: To mount the intercom, use methods compliant with local electrical codes.
Apply RTV Silicone Sealant Around Hole
Hole Plug
For Gooseneck Mounting with Optional Shroud
Remove Hole Plug Assembly prior for Shroud Installation
Washer
Nut
Network Cable (Not Provided)
Faceplate & PCB Assembly
Faceplate Mounting Screw (6x)
161019 Nut (to Ground Lug Inside 611104B)
(121017A) Washer & Nut x 3
Ground Cable (Not Provided)
611104B 3-Gang Box
Apply RTV Silicone Sealant Around Conduit & Mounting Holes
011215A Weather Shroud (Sold Separate)
(121017A) 1/4" Round Head Carriage Bolt (3x)
Gooseneck (Not Provided)
Gooseneck [Cutaway View to Show Cable Routing]
Grounding Rod, Ground Cable and Clamp (Not Provided)
Network Cable in

Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   ```
   in.tftpd -l -s /tftpboot/your_directory_name
   ```

B.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download at:

`http://www.cyberdata.net/support/voip/solarwinds.html`

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File/Configure/Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, do the following:

1. Go to the following URL:

http://www.cyberdata.net/products/voip/digitalanalog/intercomkeypadv3/faqs.html

2. Go to the support page for your product, and click on the **FAQs** tab.

C.2 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation by doing the following:

1. Go to the following URL:

http://www.cyberdata.net/products/voip/digitalanalog/intercomkeypadv3/docs.html

2. Go to the support page for your product, and click on the **Documentation** tab.

C.3 Contact Information

Contact	CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.CyberData.net Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193
Sales	Sales 831-373-2601 Extension 334
Technical Support	The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website: **http://www.cyberdata.net/support/contactsupportvoip.html** Phone: (831) 373-2601, Ext. 333 Email: support@cyberdata.net
Returned Materials Authorization	To return the product, contact the Returned Materials Authorization (RMA) department: Phone: 831-373-2601, Extension 136 Email: RMA@CyberData.net When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. No product will be accepted for return without an approved RMA number. Send the product, in its original package, to the following address: CyberData Corporation 3 Justin Court Monterey, CA 93940 Attention: RMA "your RMA number"
RMA Status Form	If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address: **http://www.cyberdata.net/support/rmastatus.html**

C.4 Warranty

CyberData warrants its product against defects in material or workmanship for a period of two years from the date of purchase. Should the product fail within the warranty period, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail out-of-warranty, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are in warranty but are damaged by improper modifications or abuse, will be charged at the out-of-warranty rate. Products shipped to CyberData, both in and out-of-warranty, are shipped at the expense of the customer. Shipping charges for repaired products shipped back to the customer by CyberData, will be paid by CyberData.

CyberData shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the products, loss of profits or revenues or costs of replacement goods, even if CyberData is informed in advance of the possibility of such damages.

C.4.1 Warranty & RMA Returns within the United States

If service is required, you must contact CyberData Technical Support prior to returning any products to CyberData. Our Technical Support staff will determine if your product should be returned to us for further inspection. If Technical Support determines that your product needs to be returned to CyberData, an RMA number will be issued to you at this point.

Your issued RMA number must be printed on the outside of the shipping box. No product will be accepted for return without an approved RMA number. The product in its original package should be sent to the following address:

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

C.4.2 Warranty & RMA Returns Outside of the United States

If you purchased your equipment through an authorized international distributor or reseller, please contact them directly for product repairs.

C.4.3 Spare in the Air Policy

CyberData now offers a *Spare in the Air* no wait policy for warranty returns within the United States and Canada. More information about the *Spare in the Air* policy is available at the following web address:

http://www.cyberdata.net/support/warranty/spareintheair.html

C.4.4 Return and Restocking Policy

For our authorized distributors and resellers, please refer to your CyberData Service Agreement for information on our return guidelines and procedures.

For End Users, please contact the company that you purchased your equipment from for their return policy.

C.4.5 Warranty and RMA Returns Page

The most recent warranty and RMA information is available at the CyberData Warranty and RMA Returns Page at the following web address:

http://www.cyberdata.net/support/warranty/index.html

Index

Numerics

100 Mbps indicator light 18
16 AWG gauge wire 12

A

AC voltages 2
AC voltages, intercom enclosure is not rated 13
act light 18
activate relay (door sensor) 45
activate relay (intrusion sensor) 45
address, configuration login 23
alternative power input 5
announcing a device's IP address 19
audio configuration 48
    night ring tone parameter 50
audio configuration page 48
audio encodings 4
autoprovisioning 60
    autoprovisioned audio files 62
    autoprovisioned firmware upgrades 61
    autoprovisioning autoupdate 61
    autoprovisioning enabled option 60
    autoprovisioning from DHCP 60
    autoprovisioning server (IP address) 61
    networking 60
autoprovisioning configuration 59, 60
auxiliary relay 13
auxiliary relay wiring diagram 14
auxiliary relay, 1A at 30 VDC 5

B

backup SIP server 1 32
backup SIP server 2 32
backup SIP servers, SIP server
    backups 32
baud rate
    verifying 18

C

call button
    indicator light 11
changing
    the web access password 26
Cisco SRST 32
command interface 66
commands 66
concrete wall mounting option (not provided) 80
conduit mounting option (not provided) 79
configurable parameters 25, 27, 30, 32, 64
configuration
    audio 48
    default IP settings 21
    door sensor 43
    intrusion sensor 43
    SIP 31
    using Web interface 21
configuration home page 23
configuration page
    configurable parameters 25, 27, 30
connector functions 15
connector locations 15, 16, 17
contact information 84
contact information for CyberData 84
current network settings 30
CyberData contact information 84

D

default
    gateway 21
    intercom settings 87
    IP address 21
    subnet mask 21
    username and password 21
    web login username and password 23
default gateway 21, 30
default intercom settings 20
default IP settings 21
default login address 23
device configuration 26
    device configuration parameters 60
    the device configuration page 59
device configuration page 26, 35, 36
device configuration parameters 27
device configuration password
    changing for web configuration access 26
DHCP Client 4
DHCP IP addressing 30
dial out extension (intrusion sensor) 45
dial out extension strings 40
dialout call 40
dimensions 5, 6, 71

pcb dimensions and intrusion sensor range 8, 74
shroud dimensions and mounting hole locations 6, 72
unit dimensions and intrusion sensor range without the gang box 7, 73
unit dimensions—front and side view 6, 71
unit dimensions—rear view and mounting hole locations 71
discovery utility program 23
DNS server 30
door sensor 43, 45, 50
activate relay 45
door open timeout 45
door sensor normally closed 45
flash button LED 45
play audio locally 45
DTMF tones 40
DTMF tones (using rfc2833) 40
dual speeds 18

E

electric screwdriver 78
enable night ring events 55
ethernet I/F 5
event configuration
enable night ring events 55
event configuration page 54
expiration time for SIP server lease 33, 42

F

factory default settings 20
how to set 20
fastening, gang box 78
firmware
where to get the latest firmware 63
flash button LED (door sensor) 45
flash button LED (intrusion sensor) 45

G

gang box, fastening 78
gasket, avoid over-torque damage 78
goose neck mounting option (not provided) 81
green link light 18

H

home page 23
http POST command 66
http web-based configuration 4

I

identifying your product 1
indicator light 11
installation, typical intercom system 2
intercom configuration
default IP settings 21
intercom configuration page
configurable parameters 32, 64
intrusion sensor 43, 45
activate relay 45
dial out extension 45
flash button LED 45
play audio locally 45
intrusion sensor range 73
IP address 21, 30
IP addressing 30
default
IP addressing setting 21

J

J3 terminal block, 16 AWG gauge wire 12

K

keypad configuration page 35

L

lease, SIP server expiration time 33, 42
lengthy pages 47
link light 18
Linux, setting up a TFTP server on 82
local SIP port 32
log in address 23

M

MGROUP

MGROUP Name 47
mounting 70
additional mounting options 79
concrete wall mounting option (not provided) 80
conduit mounting option (not provided) 79
goose neck mounting option (not provided) 81
illustration of intercom mounting process 70
mounting an intercom 70
mounting components (part of the accessory kit) 70
network cable entry restrictions 76
overview of installation types 75
rear conduit network cable entry restrictions (with shroud) 76
rear conduit network cable entry restrictions (without shroud) 76
securing the intercom 78
service loop cable routing 77
mounting components (part of the accessory kit) 70
multicast configuration 46
Multicast IP Address 47

navigation (web page) 22
navigation table 22
network activity, verifying 18
network cable entry restrictions 76
network parameters 29
nightring tones 47
Nightringer 12
nightringer settings 42

O

operating temperature 5
orange link light 18
output 5
overview of installation types 75

P

packet time 4
pages (lengthy) 47
part number 5
parts list 9
password
for SIP server login 32
login 23
restoring the default 21
payload types 5
pcb dimensions and intrusion sensor range 8, 74
play audio locally (door sensor) 45
play audio locally (intrusion sensor) 45
point-to-point configuration 34
port
local SIP 32
remote SIP 32
POST command 66
power input 5
alternative 5
power screwdriver 78
priority
assigning 47
product
configuring 21
parts list 9
product features 3
product overview
product features 3
product specifications 5
supported protocols 4
supported SIP servers 4
typical system installation 2
product specifications 5
protocol 5
protocols supported 4

R

rear conduit network cable entry restrictions (with shroud) 76
rear conduit network cable entry restrictions (without shroud) 76
reboot 64, 65
regulatory compliance 5
remote SIP port 32
reset test function management button 19
resetting the IP address to the default 70
restoring factory default settings 20, 87
restoring the factory default settings 20
return and restocking policy 86
ringtones 47
lengthy pages 47
RJ-45 15
RMA returned materials authorization 84
RMA status 84
RTFM button 19
RTFM jumper 19, 20
RTP/AVP 4

S

sales 84

securing the intercom 78
security code 40
sensor setup page 44
sensor setup parameters 43
sensors 45
server address, SIP 32
service 84
service loop cable routing 77
setting up an intercom 12
settings, default 20
shroud dimensions and mounting hole locations 6, 72
SIP
    enable SIP operation 32
    local SIP port 32
    user ID 32
SIP (session initiation protocol) 4
SIP configuration 31
    SIP Server 32
SIP configuration parameters
    outbound proxy 32
    registration and expiration, SIP server lease 33, 42
    user ID, SIP 32
SIP registration 32
SIP remote SIP port 32
SIP server 32
    password for login 32
    SIP servers supported 4
    user ID for login 32
SIP settings 32, 33
Spare in the Air Policy 85
SRST 32
static IP addressing 30
Stored Network Settings 30
subnet mask 21, 30
supported protocols 4

T

tech support 84
technical support, contact information 84
terminal block, 16 AWG gauge wire 12
TFTP server 4, 82
triggering a dialout call or security code 40

U

unit dimensions and intrusion sensor range without the gang box 7, 73
unit dimensions—front and side view 6, 71
unit dimensions—rear view and mounting hole locations 71
upgrading to firmware 6.x.x from 5.x.x 78
user ID
    for SIP server login 32
username
    changing for web configuration access 26
    default for web configuration access 23
    restoring the default 21

V

verifying
    baud rate 18
    network activity 18
    network connectivity 18

W

warranty 5, 85
warranty & RMA returns outside of the United States 85
warranty & RMA returns within the United States 85
warranty and RMA returns page 86
warranty policy at CyberData 85
web access password 21
web access username 21
web configuration log in address 23
web page
    navigation 22
web page navigation 22
web-based intercom configuration 21
wget, free unix utility 66
Windows, setting up a TFTP server on 82

Y

yellow act light 18
yellow link light 18